GENERAL PRACTICE SOLUTIONS
EXPERTLY NAVIGATING SUCCESS

71-75 Shelton Street, London, WC2H 9JQ | www.generalpracticesolutions.net
020 8865 1942 | enquiries@generalpracticesolutions.net

# COMPUTER, INTERNETAND EMAIL USE POLICY



## INTRODUCTION

GPS computers and IT network are invaluable resources which must be used appropriately

The internet offers access to almost infinite sources of information.

Email offers a fast, inexpensive, and convenient way to communicate both inside and outside the GPS and its client providers.

GPS wishes to ensure that these resources are used responsibly and productively.

Workers who work remotely, for example from home, or who bring their computers (or other devices, for example mobile telephones or tablets) into work or access work-related data on them should also adhere to his policy.

This policy should be read in conjunction with the GPS data protection policy and use of social media policy.

## APPLICABILITY

The policy applies to all employees and also applies to other people who work for GPS e.g. self-employed workers, temporary workers and contractors and who have access to the GPS or client provider computer systems.

## THE POLICY

**Computer access:**

You must keep your username/password confidential and must not divulge these to anyone. A lost or forgotten username or password must be reported to the FWO.

If you think your username/password may be known to someone else, notify the FWO immediately.

It is illegal under the Computer Misuse Act ('the Act') to steal or guess someone's username/password and to use this information to access, modify or delete data which you are not authorised to access, or to alter settings on a computer or otherwise affect its operation. It is also an offence under the Act to use someone's username/password to access a computer through which to commit other illegal acts such as 'hacking' into someone's bank account and stealing funds. Offences under the Act carry penalties of imprisonment and/or a fine.

If you are suspected of any such offences the GPS Disciplinary Procedure will be invoked. If after investigation it comes apparent that you have offended under terms of the Act, prosecutions may be brought.

**The internet:**
All workers have access to the internet.

Internet access to be solely for business use.

You must not create personal web pages or web logs ('blogs') using GPS time and resources.

You must not visit social networking websites such as (but not limited to) Facebook, MySpace, Bebo, Twitter, YouTube during GPS time.

You must not surf for or download unsuitable (especially pornographic) material.

Suitable anti-spyware, adware, anti-phishing, worm, trojan and any other appropriate protection software must be kept up to date and not circumvented.

You must not engage in activities of questionable legality (e.g. gambling).

Any material downloaded from the internet must be checked for viruses.

Any copyright, licence or usage terms on material or software downloaded from the internet must be observed.

Any licence or usage fees due on material or software downloaded from the internet must be paid (prior authorisation for the expenditure must be obtained).

Secure transactions must be used for any purchases over the internet.

Internet usage may be monitored to ensure compliance with the Policy.

Penalties for mis-use include withdrawal of access and if necessary the implementation of the GPS Disciplinary Procedure.

If, in your own time, you create your own blog or place information on social networking sites, You Tube, or any other publicly available location on the internet, it will be a disciplinary matter if you make any direct or indirect reference to the GPS or its client providers.

**Email**
Usage of external email to be solely for business purposes.

Incoming emails and any attachments must be checked for viruses/automatic virus checking must not be circumvented. Anti-virus software must be kept up to date.

Emails (both internal and external) must not contain unsuitable information or attachments e.g. defamatory/discriminatory/bullying/harassing material or comments.

All emails sent externally must include a standard disclaimer (an example is shown at the end of this policy.

Any confidential information (especially patient identifiable information) sent in an email must be encrypted.

You must not reveal or publicise confidential or proprietary information about GPS.

You must not represent personal opinions as those of GPS.
Care must be taken in addressing emails (especially when using 'copies to', address books and distribution lists) to ensure that emails are sent only to the intended recipients.

You must not access, change, or use another person's username/password/email account or files for which you do not have explicit authorisation.

Email usage and content may be monitored to ensure compliance with the Policy.

Penalties for misuse include withdrawal of access and if necessary, the implementation of the GPS Disciplinary Procedure.

**Use of personal devices**

If a worker wishes to use their own device for work-related activities, they should contact the FWO in writing with the name and model of the device and the purpose for which it is intended to be used.

Before using their own device for work-related purposes, the worker must ensure that they use a strong password to lock their device. The device must be capable of locking automatically [and deleting data automatically] if an incorrect password is entered after several attempts [or if the device is inactive for one month. Workers must know exactly what data might be deleted automatically.

Use encryption software on their devices to store personal data securely.

Ensure that if they transfer data (either by email or by other means), they do so via an encrypted channel (for example a VPN for individual services).

Ensure that they assess the security of any open network or wi-fi connection (workers should not use unsecured wi-fi networks).

Not download unverified or untrusted apps that may pose a threat to the security of the information held on their devices.

Not, under any circumstances, use corporate personal information for any purpose other than for their work and as directed or instructed by GPS.

Use different applications for business and personal use.

Ensure that they have a system of software in place for quickly and effectively revoking access that a user might gain to a device in the event of loss or theft.

Make sure that any software that they use is genuine software installed under an appropriate licence agreement between the worker and the relevant manufacturer to prevent any security vulnerabilities.

Report the loss or theft of a device used for work-related activities immediately to the FWO.

Report data breaches of which they become aware to the FWO immediately.

When accessing any document on the client provider / GPS server, workers must always log out of the [server/network/private cloud] between sessions.

Not, under any circumstances, use public cloud-based sharing or public back-up services without prior authorisation from the FWO.

Not download or access certain applications or types of data that require the identification of the workers location or an additional level of authentication.

The worker must ensure that their device is subject to mobile-device management so that if the device is stolen, upgraded, recycled for money or given to family or friends, the worker is able to locate the device remotely and delete data on demand. The worker must limit the purpose of mobile-device management to the detection of the device and the remote deletion of data. If the device is stolen, the worker must be able effectively to wipe any confidential data on the device immediately by way of a remote "locate and wipe" facility.

If workers require any technical support with their devices, they should ensure that the third party providing such support has access to any data insofar as is necessary to complete his/her work and that data is not transferred to a third-party device unless there is no other way of rectifying the technical problem. If data is transferred to a third-party device, the third party must warrant, and the worker must ensure, that the information is removed permanently from such third-party device once the problem has been rectified.

Workers must not retain personal data for longer than is necessary for the purpose for which it is being used unless there is a requirement to retain it for longer to comply with any legal obligation. If a worker is in any doubt, they should contact the FWO.

Workers must ensure that if they delete information, it is deleted permanently rather than left in the device's waste-management system. You may need to use overwriting software to achieve this. However, this is not always practicable because, for example, the information is stored or categorised with other information that is still live. In these circumstances, it is sufficient for the worker to put the information "beyond use";

This means that the worker must:

- Ensure that they do not use the personal information to make any decision that affects an individual or in a manner that affects an individual in any way.
- Not give any other access to the personal data in any way.
- Surround the personal data with appropriate technical and practical security.
- Commit to the permanent deletion of the information if and when this becomes possible.

If a worker uses removable media, for example a USB stick, to transfer personal data, they must ensure that the personal data is deleted once the transfer is complete.

Any individual whose personal data is held by GPS has the right to make a subject access request (see the GPS's Data Protection Policy for more information). This means that, if an individual makes a subject access request, then GPS may need to access your device to retrieve any data that is held on it about the individual.

You must allow GPS to access the device and to carry out a search to find any information about the individual held on the device.

Workers must ensure that if family or friends use their devices, they are unable to gain access to any personal information that is work-related by, for example, password-protecting it.

If a worker leaves GPS, they must delete all work-related personal data on their own device prion their date of GPS business.



**DATA PROTECTION**

GPS is the data controller in relation to work-related personal data that is held on personal devices. Mr Shaun Chadwick is GPS's data protection officer and is responsible for the implementation of this policy. If a worker has any questions about data protection in general, this policy or their obligations under it, they should direct them to the FWO.

The General Data Protection Regulations 2018 requires GPS to process any personal data in accordance with the six data protection principles (see the GPS Data Protection Policy). "Processing" includes obtaining personal information, retaining, and using it, allowing it to be accessed, disclosing it and, finally, disposing of it. The sixth data protection principle requires GPS to ensure that personal data is protected by appropriate technical and practical measures

against unauthorised or unlawful processing or disclosure, and against accidental loss, damage, or destruction.

Workers may store special category data on a personal device only if the device has a sufficiently high level of encryption.

**MONITORING**

As part of its ongoing obligations under the GDPR, GPS will monitor data protection compliance in general and compliance with this policy, in particular [in accordance with an impact assessment that GPS has carried out to ensure that monitoring is necessary and proportionate]. This monitoring is in GPS's legitimate interests, to ensure that the policy is being complied with, and to ensure that GPS is complying with its legal obligations under the GDPR.

Monitoring will normally be conducted by members of the FWO. The information obtained through monitoring may be shared internally, including with members of the HR team, your line manager, managers in the business area in which you work and IT workers if access to the data is necessary for performance of their roles. However, information would normally only be shared in this way if GPS has reasonable grounds to believe that this policy has not been followed.

The information gathered through monitoring will be retained only long enough for any breach of this policy to come to light and for any investigation to be conducted. Data is normally securely destroyed after six months depending on reasons for monitoring.

Workers have a number of rights in relation to their data, including the right to make a subject access request and the right to have data rectified or erased in some circumstances. You can find further details of these rights and how to exercise them in the GPS Data Protection Policy. If workers believe that the GPS has not complied with their data protection rights, they can complain to the Information Commissioner.

"Special category data" is information about an individual's:

- Racial or ethnic origin.
- Political opinions.
- Religious beliefs or philosophical beliefs.
- Trade union membership (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992).
- Physical or mental health or condition (including genetic or biometric data).
- Sex life or sexual orientation.

Information related to criminal records and convictions is also treated as special category data for the purposes of this policy.

**CONSEQUENCES OF NON-COMPLIANCE**

If a worker is suspected of breaching this policy, GPS will investigate the matter under its disciplinary procedure. If any breaches are established, this could result in disciplinary action up to and including dismissal. A worker may also incur personal criminal liability for breaching this policy.

**EMAIL DISCLAIMER**
The following disclaimer must be appended to every external email sent from GPS.

**E-MAIL DISCLAIMER - IMPORTANT INFORMATION**
The contents of this e-mail are confidential and protected by copyright. The email is intended for the named addressee only. If you are not the named addressee (or a person acting on behalf of and with the authority of the addressee) and have received this e-mail by mistake any copying, disclosure, or dissemination of the contents of this e-mail to any third party is strictly forbidden by the sender. If you have received this e-mail in error, please contact the sender immediately by return of e-mail (xxx@xxxxx.xxx.xx) and then delete this e-mail and destroy any copies thereof. Please also note that GPS endeavours at all times, to keep its network free of viruses. You should, however, scan this e-mail and any attachments to it for any viruses. GPS will not be held responsible for any viruses which may be transmitted upon receipt of this e-mail or the opening of any attachment thereto. Unless otherwise stated, any views or opinions presented are solely those of the author and do not necessarily represent those of GPS. Emails may be monitored.