Appropriate Use of Electronic Communications and Information Systems

Procedure

Greater Manchester Police

13 October 2014

Table of Contents

1. Introduction and Background

This procedure supports the Information Security Policy and aims to protect the confidentiality, integrity, availability and security of information received and stored by GMP, its information technology systems and all forms of electronic communications.

Communication and information play crucial roles in policing, supporting us in communicating with colleagues, partners, the public and other stakeholders. In order to maintain and protect the reputation of the Force and support operational policing, it is essential that GMP's data and systems are appropriately protected at all times.

Inappropriate use of information and Information Technology (IT) systems can compromise the integrity of GMP, jeopardise the prevention and detection of crime and impact on public confidence. It can also result in criminal and/or misconduct proceedings and potential dismissal for the individual concerned.

This procedure makes it clear what is and what is not permitted and outlines the responsibilities of staff, line managers and those who monitor information security, integrity, systems and professional standards.

2. Scope

This procedure applies to anyone who accesses the GMP network.

This definition includes, but is not limited to:

- Police officers;
- Police staff;
- Contractors working for and on behalf of GMP;
- GMP volunteers;
- Visiting police officers and staff;
- Partners with access to the GMP network;
- Third party suppliers;
- Researchers; and
- Work experience students.

For the purpose of this procedure, IT systems include, but are not limited to:

- Workstations, PCs and Laptops;
- Email and Faxes;
- Transportable media e.g. USB Pen Drives, CDs;
- Telephones (land-line and force issued mobiles);
- Personal Digital Assistants (PDAs), including iPADs and force issued Blackberries;
- Servers;
- CCTV images (including body worn cameras)
- Airwave radios.

3. Roles & Responsibilities

It is the responsibility of each individual to deal with information properly and ensure that their use of electronic communications and information systems is appropriate.

Each individual should ensure that they act in accordance with the standards laid out in this procedure document and all other associated internal and external documents listed in Section 6, in a way which maintains the reputation of GMP.

Any action that brings professionalism and integrity into question will be dealt with through the appropriate criminal and/or disciplinary processes.

4. Terms and Definitions

GMP standard terms and definitions are used throughout this document. Where terms and definitions are specific to a particular subject, they are listed within the appropriate section.

A **policing purpose,** as registered with the Information Commissioners Office, is: "The prevention and detection of crime; apprehension and prosecution of offenders, protection of life and property; maintenance of law and order; also rendering assistance to the public in accordance with force policies and procedures."

5. Procedure

5.1 Principles

The information stored on GMP's information systems should always be dealt with appropriately (i.e. as per the definition of a policing purpose shown in Section 4) in accordance with its level of sensitivity and commensurate with its protective marking.

The GMP network is accredited to a government protective marking of RESTRICTED. As a consequence, information at a protective marking level of CONFIDENTIAL and above should not be processed on the network.

Certain applications on the network are operating at a protective marking of CONFIDENTIAL and these have been risk-assessed with additional security measures implemented to allow data to be processed within these specific applications.

To protect the information on our IT systems, we need to maintain the confidentiality, integrity and availability of the information, by:

- protecting sensitive information from unauthorised disclosure;
- safeguarding the accuracy and completeness of information;
- making information and vital services available to users when required, giving due consideration to GMP policies and procedures.

5.2 Standards expected – Work Use:

GMP expects all use of electronic communications and IT systems to conform to the highest professional standards:

- To be accurate, complete and timely;
- To be appropriately secure;
- To be shared only when appropriate;
- To be in accordance with legislative requirements, Government guidelines and good practice;
- To avoid behaviour, actions, language or images which could be considered to be discriminatory or offensive to an individual or group of people;
- Only use Force-approved transportable media when absolutely essential. It should not be used as a matter of course.

All staff must:

- Ensure that all information is marked in accordance with the Government Protective Marking Scheme;
- Ensure that all information entered onto GMP and other relevant / approved systems is as accurate as possible – the quality of information has a direct impact on policing and public confidence;
- Comply with Authorised Professional Practice and the Data Protection, Copyright, Designs and Patents and Computer Misuse Acts;
- Ensure that access to information is controlled in accordance with legislative requirements and information is shared only when appropriate to do so;
- Ensure that information is protected and kept securely, with adequate precautions taken against theft, loss, damage, destruction or misuse of data;
- Comply with all procedures for the IT systems they use;
- Report any suspected breaches of Information Security through their manager or supervisor;
- Take particular care with information they are authorised to access, particularly information on any transportable media and information available in printed form – the harm resulting from wrongful disclosure or misuse can be extremely damaging;
- Take necessary steps to ensure as reasonably possible, duplication and inaccuracies are avoided when entering information onto information systems;
- Read all relevant further information contained within the Appendices, follow all published guidance and action as appropriate.

5.3 Standards Expected – Personal Use

GMP IT and communications systems are provided for use in the course of, or in connection with, GMP business. However, GMP does permit limited and reasonable personal use of GMP telephone and email systems and access to the Internet. It is important that on these occasions, access to the systems:

- Are only outside working hours (i.e. in breaks/refreshment breaks or before or after recorded working hours);
- Will not negatively affect the reputation of GMP or public confidence; and
- Are in accordance with the guidance and standards laid out in this document.

In addition to the above, legitimate personal usage should be:

- Reasonable in terms of amount of time spent;
- Justifiable in terms of cost (if any) being met from public funds;

Work-based use of IT systems should take priority over personal use, e.g. the use of streaming media such as video broadcast, is putting severe strain on the capacity of GMP systems. Staff should consider using electronic or IT systems other than those of GMP for personal purposes as far as possible.

Facebook and other social media networks should only be used for authorised work related use (see Appendix E for more details).

If challenged, staff should be able to justify their use of GMP equipment and systems.

Any conduct that breaches criminal law or GMP's Information Security Policy will be dealt with accordingly.

5.4 Monitoring

GMP has the right to monitor the use of its IT systems and electronic communications.

Lawful Business Monitoring allows a business to monitor, without consent, and to keep records of communications:

- In the interests of national security;
- To prevent or detect crime;
- To investigate or detect unauthorised use of telecommunications systems; or
- To obtain evidence of the communications
  - To establish the existence of fact;
  - To ascertain compliance with practices or procedures; or
  - To ascertain or demonstrate standards such as quality assurance.

In order to meet the requirements set out in the Data Protection Principle 7 and to address the threats highlighted by ACPO and SOCA, GMP have chosen to overtly deploy 3ami Monitoring and Auditing Software (MAS).

3ami will also allow the System Controller to monitor and keep a record of activity on GMP computer systems for the purpose of preventing and detecting crime.

GMP will examine the content of business and personal communications when it is necessary, justified, proportionate and authorised by Chief Superintendent, Professional Standards Branch.

When using GMP systems and electronic communication, staff should not automatically expect privacy and be aware that the information they communicate may be monitored.

Appendix A contains general information about communications that are routinely monitored, personal privacy, emails, internet, telephones plus guidance about intrusive monitoring for line managers. It is advised that all staff familiarise themselves with this information.

5.5 Passwords

User identity numbers (PIN numbers) and passwords are the main method of authenticating staff onto our systems. Your password identifies you and staff should not reveal their password to anyone else.

There should be no occasions when staff have to use someone else's PIN/UserID and password to carry out their duties. Staff will be held responsible for any activity conducted under their own account. If you believe there are circumstances which require you to divulge your password to a third party, you must contact the Information Security Manager for advice before doing so.

Appendix B contains advice on selecting passwords, changing passwords, plus advice and guidance for line managers to ensure correct levels of access for staff. It is advised that all staff familiarise themselves with this information.

5.6 Use of GMP Electronic Mail (email)

All GMP staff should ensure that their email account is activated and available for use at the earliest possible opportunity after appointment, and that once activated they check their account at regular intervals.

There is a requirement for staff to manage their email accounts by regularly deleting any emails no longer needed for GMP business. The retention period for information will be dependent on the purpose for which it is held. Information should be retained and disposed of in accordance with the Force's Retention and Disposal Schedule.

All unwanted emails over 90 days old are to be deleted from mailboxes. When using the delete button, emails are transferred to the "Trash Folder" or the "Deleted Items Folder". The contents of these folders should also be deleted, thereby complying with the Information Commissioners guidance on the double deletion of emails.

Emails may be subject to disclosure under the Freedom of Information (FOI) Act and as such a FOI request could open up an email trail. It is therefore important to ensure that email management is undertaken and that everyone should consider the need to only add to an email if it adds value to the subject.

Guidance on how to use email appropriately, effectively and in the corporate style can be found in the 'Making Connections Toolkit' produced by the Corporate Communications Branch.

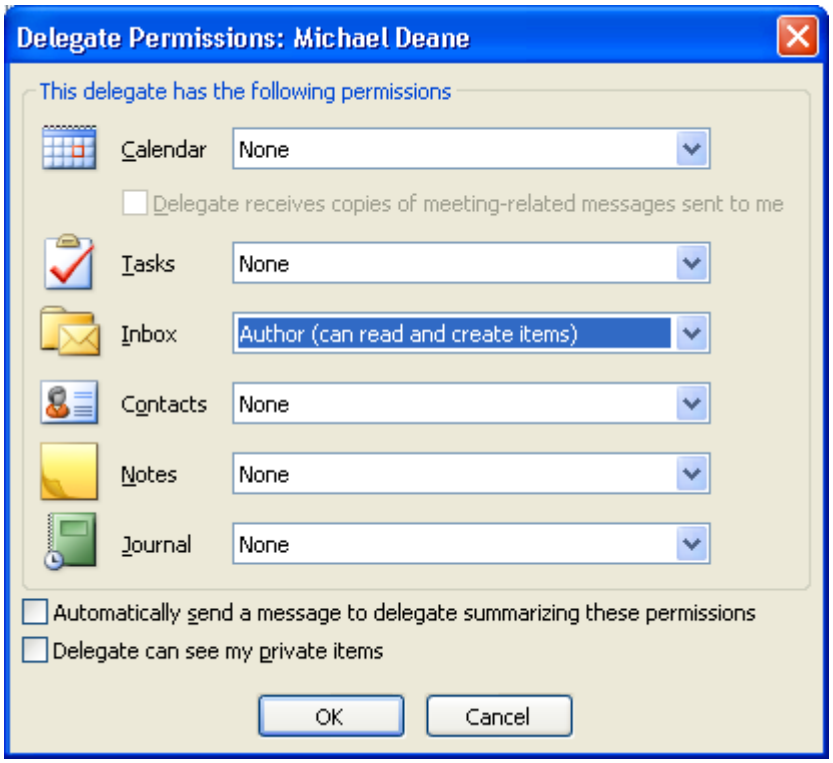
If using the email system to send/receive personal emails (in accordance with the standards set out in paragraph 5.3 of this procedure) staff should be aware that the email system cannot differentiate between personal and business emails and personal emails cannot be afforded any degree of privacy. A disclaimer to this effect

will appear on emails sent. However if staff are in the habit of receiving personal emails, they should make the senders aware that their emails will be recorded and monitored.

All staff:

Providing access to your e-mail WITH the account holder's permission:

Staff should set up their e-mail accounts and nominate their line manager to have access, so that in the event of unplanned absence he/she can deal with any e-mail correspondence.

Step	Procedure
1	**If you have a Lotus Notes Account**, open your account and select: • Actions>More>Preferences>Access & Delegation Tab>Add Tab> • On Select Name Window, select GMP's Address Book and search for your Line Manager and Double Click on their named entry> • In Components box, select: Mail, Calendar, To Do and Contacts> • In Access Box, select: Read, Edit, Create and Send, Enable Out Of Office> • Click OK>Click OK.
or 1	**If you have a Microsoft Outlook Account**, open your account and select: • File tab>Account Setting>Delegate Access>Add> • In the Add Users box Search for, select and Add your Line Manager>Click OK> • Then complete the Delegate Permissions Box as below: 

If you know you will be absent for some time and wish others to have access to your e-mails, you should amend the Access Control List (ACL) on your mail file or use the 'delegation profile' to allow named individuals access to your account.

All Line Managers:

If a member of your staff is absent and has not set up an "out of office" response, you should open his or her e-mail account and set up the response. Deal with any outstanding correspondence in the person's inbox if appropriate to do so.

Access to an e-mail WITHOUT the account holder's permission:

There are circumstances in which someone else, usually a member of staff's own line manager, or another manager, can legitimately open their GMP e-mail account. This is known as third party access. This procedure explains how GMP will authorise such access and who will be allowed access. The same procedure also covers access to the 'personal' area of the network, known as the 'Y' drive or PIN data area.

There may be a requirement to ensure that personnel can legitimately access another person's mailbox. For instance, requesting access to a Notes or Outlook account when the account holder is ill or on extended leave. The procedure for accessing mail boxes and/or the 'Y' drive or PIN data area is contained in the table below.

Every access request will be assessed on its own merits. This procedure does not give line managers authority to access data indiscriminately.

Step	Procedure
1	If you think there is a legitimate need to gain access to an account in any circumstance, you should ask for advice from the Customer Services Desk on 61400. When requesting access, you should be aware that the decision whether to grant or refuse access will depend on: • the urgency or importance of the work; • the relevance of the current business need; • the expected duration of the account holder's absence; and • the availability of other suitable measures, such as asking the sender to send the e-mails to another person.
2	The person making the access request must then confirm the details in writing by e-mail to the Customer Services Officer dealing with the access request and ensure that it is accompanied by the required authorisation from a Senior Manager of at least Superintendent or Assistant Director level.
3	The Customer Services Officer dealing with the access request should then send a written report, together with the required accompanying authorisation to the Assistant IS Director (Operations) stating the period for which access is required. If the Assistant IS Director (Operations) is absent, the report can be sent to any member of the IS Branch Senior Management Team. Customer Services Staff will not give access in response to a request made by telephone.
4	Assistant IS Director (Operations): If the request is approved, you should inform staff in the Customer Services Team by e-mail. They will enable

	access to the account.
5	If the account holder returns to work before the period of permitted access has expired, the person who made the original request should telephone Customer Services Desk on 61400 and tell a member of the Team to have the access permission revoked.

Email Calendar

As part of the email functionality there is a calendar application. This application allows, amongst other functions, calendars to be interrogated for purposes such as booking meetings, etc. The default for the calendar function will be allow “all” to view.

If there is something in a staff member’s calendar that they do not wish everyone to view, they can use the “private” function when they originate the entry.

Automatic forwarding to private email addresses

The automatic forwarding function in Lotus Notes is NOT to be used within GMP. Automatic forwarding provides no control over what is being forwarded. Similarly rules are not to be set in Outlook that forward messages to a non-GMP address.

Appendix C contains further information on use of email, sending emails outside the European Economic Area and SPAM or hoax emails. It is advised that all staff familiarise themselves with this information.

5.7 Use of Internet

All personnel can access the Internet with a valid user ID/password and from any workstation. The use of the Internet must be commensurate with your duties and must be justifiable. GMP will not tolerate the use of GMP equipment for any inappropriate activity such as downloading offensive documents, text or images. If you are in any doubt about a course of action, take advice from your line manager.

Staff may make occasional and reasonable personal use of the Internet, but only where that use:

- is only outside working hours (i.e. in breaks/refreshments breaks or before or after recorded working hours); and
- complies with the standards set out in this procedure.

Where these conditions are not complied with, the right of personal use will be withdrawn and the misuse or abuse may result in action under the disciplinary procedure being instigated.

Overt use of internet

Staff should be aware that when visiting an Internet site from a GMP workstation, the site might log the fact that they are located at GMP. Any activity that they engage in may therefore affect GMP. Any staff or teams wishing to covertly access the Internet need to be aware of this fact as it may compromise their operations. Further advice on covert access should be obtained from the FIB Covert Section.

Internet monitoring

All Internet activity is monitored or logged by GMP and monthly reports are produced. Where misuse is suspected or noted, the relevant Branch/Divisional contact is notified.

Appendix D contains further information on Appropriate Internet Access and what staff should do if they require access to a blocked site for a policing purpose. It is advised that all staff familiarise themselves with this information.

5.8 Use of Social Networking Sites

Social networks are online services or sites that are focused on building networks or relationships with people online, either professional or social. Social networking sites allow people to share ideas, activities and interests with other people on the network, and engage in conversations about topics of interest to them. Social networking sites include, but are not limited to, Facebook, Twitter, YouTube, Flickr, MySpace, Bebo, Uniformdating and Friendster.

GMP does not allow access to social networking sites from its systems at any time, unless previously authorised for policing purposes. The Force Media and Social Media Communications Policy and Procedure and Social Media Procedure covers official use of social media.

This procedure also covers Police Officers and Staff when using social networking sites personally, when not at work, but who publicly declare an association with GMP in their employment or otherwise. For example, references to it through friendships, updates or photographs which may unwittingly put their employment at risk or bring the Force into disrepute by their activity.

GMP respects an employee's right to a private life. However, GMP must also ensure that confidentiality, integrity and its reputation are protected. It therefore requires Police Officers and Staff using social networking websites to:

- Ensure they do not conduct themselves in a way that it is detrimental to GMP;
- Take care not to allow interactions on these websites to damage GMP's reputation, working relationships between colleagues, members of the public or other organisations;
- Not upload any data from GMP's systems, for example, CCTV footage;
- Consider if it is appropriate to identify themselves as working for GMP. All Police Officers and Staff have a responsibility to consider the impact of their actions in and outside work that may impact upon GMP's reputation, values and their own position. All Police Officers and Staff who knowingly or inadvertently declare a connection with GMP as their employer or otherwise, need to be aware of the personal and corporate risks before making an informed decision on their social networking activity.

Appendix E contains further information and advice on Security, Personal Risks and Unacceptable Content. It is advised that all staff familiarise themselves with this information.

5.9 Use of GMP Telephones and Faxes

GMP provides telephones (both fixed and mobile) and fax facilities for use by its staff in the course of, or in connection with, GMP business.

GMP recognises that it is sometimes necessary for staff to deal with personal or welfare issues during the working day and as such will allow limited personal use from GMP fixed phones. This must be notified to the line manager at the first available opportunity.

Mobile phones can be used for personal use but personnel must reimburse GMP for the personal calls.

GMP telephone and faxes are not to be used for:

- unlawful activities;
- personal financial gain;
- commercial purposes;
- any other activity that would constitute an act of misconduct.

5.10 Use of GMP Airwave Radios

Airwave is a sophisticated and complex radio system. The introduction of Airwave terminals has provided encryption, but care should still be taken to avoid the transmission of any information that may be of use to unauthorised persons who may overhear messages.

GMP radios are not to be used for:

- unlawful activities;
- any other activity which would constitute an act of misconduct.

All users should read GMP's Airwave Policy and Procedures, which provide guidance for good working practices and should be adhered to for the benefit of all users.

If any member of staff discovers or suspects that a radio is lost or stolen, they must report the matter immediately to their supervisor, Radio Custodian and subsequently to Radio Network Services (during normal working hours) or the Force Duty Officer (out of hours) who will make immediate arrangements for the radio to be disabled from the system.

5.11 Use of GMP Laptops

The IS Branch provide hundreds of laptops across the Force, all of which are configured to automatically receive security patches and anti virus updates when connected to the GMP network.

Staff should connect their laptops to the network and log on at least once a month to ensure that the anti virus software is only ever one month out of date.

Laptops should be left connected to the network all day if they have not been connected for some time, as there may be many updates to install.

Further advice is available from the IS Service Desk.

5.12 Management, Issue and Audit of USB Memory Sticks

In October 2011, the Force introduced software which enforced controls on the ability to connect USB memory sticks, and potentially other device types, to GMP desktop and laptop computers. This ensures that unapproved and unauthorised USB memory sticks cannot be used and also provides extensive audit capabilities to enable the use of USB devices to be monitored.

The USB control software is configured to allow only approved encrypted USB memory sticks to be written to, i.e. staff cannot freely copy information from GMP systems to a USB memory stick. However it will allow any device to be read from. This is to facilitate legitimate access to information received on such devices from third parties.

Procedures are provided below for the following:

- Issue and use of encrypted USB memory sticks;
- Issue and use of unencrypted USB memory sticks;
- Use of USB memory sticks to view non-GMP data and
- Loss of USB memory sticks.

The steps in each procedure act as an aid to managers in deciding whether there is a justifiable case for USB memory sticks to be used and the procedure necessary to control the issue of those USB memory sticks. The purpose is to protect GMP data from compromise and/or loss. It is not intended to prohibit the legitimate business use of a USB memory stick to view non-GMP data, e.g. CCTV footage from third parties.

Definitions:

USB Memory Stick – includes pen drives, and both of these terms are part of the overall generic term of “flash drives”, exceptionally external hard drives may also be issued where large capacity is required.

Encrypted USB Memory Sticks – require a password to access the data contained on the USB Memory Stick as the data is encrypted.

Unencrypted USB Memory Sticks – do not require a password and the data can be accessed by anyone in possession of the USB Memory Stick as the data is unencrypted.

Personal Data – as defined by the Data Protection Act 1998 (i.e. data that can identify a living individual)

Delegated Authorising Officer – an individual nominated by a Branch Head/Divisional Commander to authorise the provision of USB Memory Sticks on their behalf, whilst retaining accountability for their Delegated Authorising Officer’s decisions. Any Branch Head/Divisional Commander who nominates an individual to act as their Delegated Authorising Officer should submit confirmation of their authority for this to #Information Security so that the list of authorised Approvers can

be maintained accurately. It is not essential for a Branch Head/Divisional Commander to nominate a Delegated Authorising Officer.

Issue and use of Encrypted USB memory sticks

Step	Procedure
1	In all cases, if any officer or member of staff believes that it is necessary to use a USB memory stick to undertake an essential business process they must submit a report to their line manager explaining why it is necessary for them to be issued with an encrypted USB memory stick. This must identify the business process for which the use of a USB memory stick is essential and the required duration of its use.
2	The relevant Branch Head/Divisional Commander or Delegated Authorising Officer should ensure there is an essential business need for the use of a USB memory stick: • The overarching consideration in permitting the use of a USB memory stick must be the protection of GMP information and therefore the Branch Head/Divisional Commander or Delegated Authorising Officer should ensure that any risk posed by the potential loss of the USB memory stick is mitigated; • The line manager should therefore ascertain whether the identified business need can be met via an alternative means, for example whether a change to the business process would remove the need to use a USB memory stick; • Where the USB memory stick is to be used to transfer data, the line manager should be assured that the recipient has a legitimate need to have this information. This legitimate need will be detailed in the appropriate Data/Information Sharing Policy; • USB memory sticks should not be routinely issued on a permanent basis.
3	If the request is approved and before the USB memory stick can be issued, the officer or member of staff whom requires the USB memory stick should complete and sign the Agreement document and submit it to their Branch Head/Divisional Commander or Delegated Authorising Officer.
4	The Branch Head/Divisional Commander or Delegated Authorising Officer should email #Information Security with the following details: • confirmation of their approval; • the completed Agreement detailed at 3; • the PIN of the person being issued with the USB memory stick. The recipient of the USB memory stick can then be added to the appropriate Authorisation Group and the Force USB Memory Stick Issue Log updated with the relevant details.
5	The line manager must inform the member of staff that they are

	responsible for ensuring that: • Only data that is commensurate with the approved use is retained on the USB memory stick; • All material stored on the USB memory stick should be marked in accordance with the Government Protective Marking Scheme (GPMS). In no circumstances whatsoever should any material that is GPMS marked CONFIDENTIAL or higher be recorded or stored on the USB memory stick; • As the USB memory stick has been personally issued to them, they are responsible for its security and safe use; • Under no circumstances should the USB memory stick be used by or transferred to another member of staff; • Data should not be retained on the USB memory stick any longer than absolutely necessary; • They are aware that any breach of this procedure may lead to action under GMP's disciplinary procedure and/or result in the commission of criminal offences.
6	The recipient must update the owner information fields on the USB memory stick encryption software when setting their password for the first time. The officer or member of staff must also insert their details onto the USB memory stick.
7	At the end of the authorised period the person allocated the USB memory stick must delete all data from the memory stick, including their owner information, and arrange to personally return it to IS Customer Services. You should also email and advise #Information Security of the return so that the Force USB Memory Stick Issue Log can be updated accordingly.

Issue and use of Unencrypted USB memory sticks

Step	Procedure
1	The USB control software will prevent information being written to unencrypted USB memory sticks. It will allow any device to be read from, which will facilitate legitimate access to information received on such devices from third parties.
2	The issuing of an unencrypted USB memory stick should only be approved in **very exceptional circumstances**. For example, where there is no capability to interact with the USB memory stick to enter the passwords. The risk to the Force and the individuals concerned is raised significantly when unencrypted USB memory sticks are used.
3	The process for issuing unencrypted USB memory sticks is the same as shown in the procedure for issue and use of ENCRYPTED USB memory sticks above except for the following additions: • Where USB unencrypted memory sticks must be used, the line

	manager must ensure that the recipient of the USB memory stick is aware that no personal data, as defined by the Data Protection Act 1998, can be stored on an unencrypted USB memory stick. This includes any information marked as RESTRICTED or above. Should the Branch Head/Divisional Commander or Delegated Authorising Officer be of the opinion that in complying with this the business process will be disabled then additional authority must be sought. Where this information is marked CONFIDENTIAL or higher, approval cannot be granted. • When seeking additional authority, the Branch Head/Divisional Commander or Delegated Authorising Officer should endorse the use of an unencrypted USB memory stick and forward this for the attention of the Information Security Manager, Information Services Branch. The Information Security Manager will review the request and make a recommendation to the Senior Information Risk Officer (currently ACO Resources). The Information Security Manager will notify the appropriate individuals of the decision and if authority is granted, ensure that the Corporate Risk Register is updated. • When additional authority is not required, the line manager should notify the Information Security Manager, Information Services Branch, that an unencrypted USB memory stick has been issued. • In either case, if approval to use an unencrypted USB memory stick is given, the line manager must implement additional safeguards to prevent the loss of the unencrypted USB memory stick. These are: ➢ The unencrypted USB memory stick must be secured in a locked container when not in use and access restricted to the person it is issued to; ➢ It should not leave GMP premises without express permission of the Divisional/Branch Commander if it contains GMP data; and; ➢ A record should be maintained of the location of the unencrypted USB memory stick.
4	At the end of the authorised period the person allocated the USB memory stick must delete all data from the memory stick, including their owner information, and arrange to personally return it to IS Customer Services. You should also email and advise #Information Security of the return so that the Force USB Memory Stick Issue Log can be updated accordingly.

Use of USB memory sticks to view non-GMP data

Step	Procedure
1	Where information is presented to GMP on a USB memory stick which needs to be assessed as possible potential evidence then normal evidential processes will apply and ACPO Guidelines in respect of Digital Evidence must be adhered to.

2	Where non-evidential information is presented to GMP on a USB memory stick which needs to be assessed, for example, training material, documentation for a product, softare etc. then these USB memory sticks can only be viewed on GMP computer hardware. Once viewing has been completed it may be appropriate to save the information. The introduction of USB management software supports this process by enabling such USB memory sticks to be read from but not written to.

Loss of USB memory sticks

Step	Procedure
1	In the event of any USB memory stick being lost by a member of staff, their line manager should be notified as soon as possible.
2	Force Form 514B should be completed by the person reporting the loss and returned to the Information Security Manager. This will ensure that the correct reporting process for data breaches/losses is followed.

Audit

Auditing these procedures will be incorporated within the Force Audit Plan. The Force USB Memory Stick Issue Log with details of USB recipients is subject to review and will also be made available to audit personnel on request.

Staff issued with GMP memory sticks must make them available and accessible to audit personnel on request.

5.13 Management, Issue and Use of GMP iPads

This procedure documents the current Force approach to mobile solutions which is currently strictly limited to Force-issued iPads.

This procedure covers the authorisation, issue, usage and return of GMP iPads as part of the “Tablets for Senior Officers Project”. As of March 2014, no other mobile devices are to be issued by GMP. This document will be updated as GMP device usage and/or the security threats change, therefore iPad users should keep themselves updated with changes.

Terms and definitions

iPad – refers to a GMP-sourced and issued Apple iPad.

iOS – refers to the iPad operating system, as issued and updated by Apple from time to time.

Good or **Good MDM** – refers to Secure Corporate Software and Device Management tools installed and configured on the iPad, used by GMP to enforce certain control settings and report on iPad usage.

The Good environment – refers to data and apps that are accessed by opening the Good application installed on the iPad.

Issue and Use of GMP iPads

Step	Procedure
1	In all cases, if any officer or member of staff believes that it is necessary to use an iPad to undertake an essential business process they must submit a business case to Command via their respective Chief Officer.
2	The overarching consideration in permitting the use of an iPad must be the protection of GMP information and therefore the user should ensure that any risk posed by the potential loss of the iPad is mitigated. The individual and their respective Chief Officer should therefore determine whether the identified business need can be met via an alternative means, for example whether a change to the business process would remove the need to use an iPad.
4	The iPad User is responsible for ensuring that: • Only Corporate information is stored in the Good environment; • Corporate Information stored in other applications on the iPad must not be of a sensitive nature, since it will be less well protected and managed than data stored within the Good environment; • All material accessed or stored on the iPad within the Good environment should be marked in accordance with the Government Protective Marking Scheme (GPMS); • In no circumstances whatsoever should any material that is GPMS marked CONFIDENTIAL, SECRET or TOP SECRET be processed or stored on the device; • The iPad is a personal issued device and as such, the individual is responsible for its physical security and safe operation (ensuring GMP information is properly protected in terms of confidentiality, integrity and availability); • Under no circumstances should the iPad be used by or transferred to anyone else; • Information should not be retained on the iPad any longer than absolutely necessary; • Any breach of this policy may lead to action under GMP's disciplinary procedure and/or result in the commission of criminal offences; • The device password must be alphanumeric and at least 8 characters in length • The Good application password may be as short as 4 characters.
5	At the end of the authorised period, IS Branch must be informed, and the device returned. After appropriate processes to ensure any required data is available to GMP, the iPad device will be completely wiped. IS branch will issue a receipt confirming that the user has returned the device.

Use of the iPad to view or store non-GMP data

The use of the Force-issued device for personal use is permitted, however the user should be aware that any personal use that incurs additional cost to the force, such as 3G use abroad, or exceeding the 5Gb data download with 3G in the UK, should be avoided.

Use of the iPad in public areas

The iPad, by its nature, is a mobile device intended for use outside of the confines of a GMP office. Users must therefore take appropriate steps to ensure GMP data remains secure whilst the device is in use.

Users should be aware not only of the people around them, in the immediate vicinity, but also of the wider environment. There have been numerous instances where cameras have been used to capture images of papers held in plain sight – iPads could just as easily be targeted.

The nature of the data being accessed will determine the level of care required. It may be appropriate for the user to relocate themselves or reposition the iPad to ensure privacy.

Use of the App Store

Currently all Senior officers may download applications from the Apple application store for evaluation purposes. As useful applications are identified as part of GMP's iPad Project they will be reviewed to ensure they provide appropriate security of GMP data. It is envisaged that future rollouts will provide a 'GMP app store' where approved applications can be downloaded. Most users will then be restricted to applications downloaded from the GMP app store only.

When considering applications for Force use, consideration must be given to how Force information is secured and backed up. The back up process for an application is usually well documented within the application. If the application does not provide a backup methodology, it is possible to create a workflow which ensures that a copy of the data is securely transmitted to an appropriate, secure location off the device.

When selecting applications for use with any mobile device, it is essential to consider the implications of device loss / device wiping (see 4. Good Wipe below). The device must not be used to store important or critical information unless a copy of that data is held elsewhere, other than short periods of 'temporary' storage e.g. making notes or taking photographs, until a backup is performed by the application used to capture the information e.g. Microsoft One Note which uses a Home Office accredited "Cloud" back up solution by copying any documents created whenever a network connection is available. The device should not be used to hold important or critical data that has not been backed up, unless that data can easily be recreated.

Good Wipe

The Good software provides two wipe functions: remote and local wipe. Both functions will return the device to the 'factory settings' and all user data stored on the device will be deleted. If the device is still owned by GMP after the wipe process the Good environment can be easily restored by following the initialisation instructions and reinstalling the Good applications.

Remote Wipe

The remote wipe function will be initiated by IS Branch when a user reports that a device is lost, may be lost, has been stolen, or may have been stolen. The user must report immediately if any of these cases are suspected. They should report this in the normal manner.

IS Branch will then initiate the remote wipe command. This uses the iPad's internet connection to issue the wipe command, which will result in all user data being securely deleted from the device.

If the device is confirmed as lost or stolen, it is important that Vodafone is contacted to block the SIM card. IS branch will take appropriate steps to ensure the SIM is blocked. This is to avoid any attempts to defeat or avoid the wipe command which can be done by powering the device off and removing the SIM card, before connecting it to a PC and attacking the Good encryption, whilst denying any internet connection through wireless or other connectivity. Once the Good Wipe has been performed, the SIM card will continue to function, and thus if the device has been lost or stolen, anyone could continue to incur expenses to GMP through use of the SIM card.

Local Wipe

Local Wipe is initiated by the Good app installed on the device. If it is powered up and has no internet connection, after 30 days the wipe will be initiated. The local wipe is an effective fail safe which will remove all user data from the iPad, unless it has been confirmed with the Good Network Operating Centre that no wipe command has been issued.

Please Note: Users should be aware that iPad usage for 30 days without any internet connection may result in the device being wiped.

iOS upgrades

Apple provide minor version upgrades to their operating system on an irregular schedule. Major upgrades are usually issued annually. When an upgrade is released, the settings icon on the iPad shows a red number, indicating that an action is required, and if the user clicks on *Settings*, *General* and then *Software Update,* they will see details of the update that is outstanding for their device.

Users will need to have a fully charged battery and be connected by Wifi to install the update:

- Minor version upgrades, e.g. from 7.0.5 to 7.0.6 or 7.1.0, should be installed by users as soon as they notice that the update is available.
- Major upgrades, e.g. from 7.1.0 to 8.0.1, should only be installed following advice from IS Branch.

The Information Security Team monitors iOS upgrades and investigates the reason for the upgrade. If the upgrade fixes significant security vulnerability then appropriate advice will be issued to users, requesting that they upgrade as soon as possible.

Occasionally, the Good MDM software will be used to reject access to the Good environment if a specific iOS upgrade has not been completed.

Under most circumstances, users will be given at least one week's notice of such an upgrade enforcement decision.

Appendix F contains further information and advice on Overseas use and Use of wireless networks. It is advised that staff with a GMP iPad familiarise themselves with this information.

6. Associated Documents

Internal

Information Security Policy

Data Protection Policy

Greater Manchester Police Government Protective Marking Scheme (GPMS) Procedure

3ami Monitoring and Auditing System Policy

Authorised Professional Practice – Information Management

Media & Social Media Communications Policy & Procedure

Airwave Policy & Procedure

Making Connections Toolkit, Corporate Communications Branch

External

Computer Misuse Act 1990

Data Protection Act 1998

Human Rights Act 1998

Equality Act 2010

Freedom of Information Act 2000

Regulation of Investigatory Powers Act 2000 (RIPA)

NPIA Code of Practice (CoP) on the Management of Police Information (MoPI) July 2005

NPIA Guidance on the Management of Police Information (MoPI) Second Edition 2010

7. Consultation & Statutory Compliance

7.1 Statutory Compliance

7.1.1 Data Protection Act (1998)

The use of Information Systems for processing personal or sensitive personal data is governed by the Data Protection Act 1998. The Act affords protection to data subjects (whom the information is about) by stipulating controls and safeguards that must be adhered to when handling personal information on information systems whether electronic or paper based.

The procedures set in this document comply with the Data Protection Act 1998 and in conjunction with associated documents set out controls in place for personnel accessing the GMP network.

The integrity of information stored in GMP systems is largely dependent on personnel therefore it is essential all personnel are well versed with their responsibilities and adhere to the safeguards set in this procedure and associated documents at all times to ensure the use of information systems comply with the requirements of the Act.

7.1.2 Freedom of Information Act (2000)

Upon request under the Freedom of Information Act 2000 this procedure is eligible to be assessed for disclosure and where possible exemptions from disclosure will be utilised to prevent disclosure.

7.1.3 Equality Act 2010

The procedures set out in this document have been considered in the context of the General Equality Duty. The requirement for the appropriate use of GMP electronic communications and information systems applies equally to all staff, whether or not they share protected characteristics.

8. Appendices

Appendix A: Monitoring
Introduction, Personal Privacy, Emails, Internet, Telephones, Advice for Line Managers

Appendix B: Passwords
Selecting your password, Changing your password, Advice for Line Managers

Appendix C: Use of GMP Electronic Mail (email)
Use of email, Sending emails outside European Economic Area, SPAM and hoax email

Appendix D: Use of Internet

Appropriate Internet Access

Appendix E: Social Network Sites

Security & Personal Risks, Unacceptable Content

Appendix F: Management and Issue of GMP iPads

Overseas Use, Use of Wireless Networks

Appendix A: Monitoring

Introduction, Personal Privacy, Emails, Internet, Telephones, Advice for Line Managers

Introduction

GMP uses a wide range of products to gather information for monitoring and auditing the use of systems within the GMP network.

Some communications are routinely monitored full time (for example, radio and telephone conversations in Operational Control Rooms are monitored as a matter of course) whilst others will be monitored when justified and in accordance with this procedure.

The methods of monitoring and auditing range from embedded tools in application to those specifically designed for auditing access.

Examples of these are:

- Event logs in windows applications;
- Reason code in PNC;
- 3ami for general and bespoke auditing;
- Digital Voice Recording.

Personal Privacy

This procedure is intended to take into account legislation that aims to ensure a minimum level of personal privacy for employees in their employment.

The Telecommunications Data Protection Directive requires European Union members to protect the confidentiality of communications made over a public telecommunications system.

The Regulation of Investigatory Powers Act 2000 (RIPA) fulfils the UK's obligation by making regulations to govern interception and protect confidentiality.

The directive extends:

- to all types of communication made by means of the public telecommunications network, including emails and faxes; and
- to private networks connected to the public system, such as that run by GMP.

The law prohibits listening to, tapping and storage of communications without consent except where legally authorised.

The RIPA also created regulations for lawful business monitoring that allow a business to monitor without consent and to keep records of communications for specific purposes.

An audit/monitoring tool is deployed on all computers and will capture all actions on that computer. The information will be stored and used with the authority of the Chief Superintendent Professional Standards Branch, when it is deemed necessary, justified and proportionate to lawful business monitoring purposes (e.g. in the event of a CCU investigation into suspected misuse of GMP information).

Emails

All emails received by or transmitted by GMP are routinely recorded by the GMP email system.

Details recorded are the sender, intended recipients and the subject. No other details are recorded. This is **not** intrusive monitoring.

Internet

All Internet access is logged, with the PIN/UserID being used as the source for recording these details. All sites visited by personnel are recorded.

The Information Security Team produces monthly reports and if any misuse is suspected or detected, this is forwarded to Branch/Divisional contacts for further investigation.

Telephones

The Information Services Branch records details of all telephone calls made from GMP extensions and bills are sent to Branch/Divisional contacts for checking.

All telecommunications using GMP lines are subject to monitoring in accordance with Lawful Business Monitoring RIPA.

Advice for Line managers

The approval of the Professional Standards Branch Chief Superintendent, or his or her deputy, is required for intrusive monitoring.

There may be occasions when this intrusive monitoring is not appropriate and details need to be gathered prior to intrusive monitoring being authorised. In these circumstances the approval of a Superintendent/Assistant Director should be sought and this should be forwarded to the Assistant Director (Business Operations), Information Services Branch or the Information Security Manager, Information Services Branch.

Examples of where this could be used are if line managers need to confirm that individual members of staff have been abusing the email system and you need to discover the amount of emails being sent and to whom.

When intrusive monitoring is authorised this could involve looking at email contents and attachments, computer hard drives and the personal area of the network, which is known as the PIN data area.

Appendix B: Passwords

Selecting your password, Changing your password, Advice for Line Managers

Selecting your password

When you are first issued with a password, you must change it at once. Failure to do so means that the password will be known to at least one person other than yourself.

- The password must consist of:
  - At least eight characters;
  - Letters and numbers; and
  - Upper and lowercase letters.
- To make your password difficult to guess, you should not use:
  - Common words that are found in dictionaries (most password cracking devices run a dictionary check first);
  - The word “password” or any derivative of the word “password” such as Password12 or Password75;
  - Alphabetic, numeric or keyboard sequences such as “Abcdefg34” or “A123456789” or “Qwerty789”;
  - Consecutive identical characters e.g. “Aabbcc1122”.
- You should avoid using words or terms that reflect your lifestyle, such as:
  - Names of your spouse, child or pet;
  - Car model or registration number;
  - Address or telephone number;
  - Your rank or post title;
  - Any reference to Police or GMP

The above restrictions may appear to make it difficult to choose a password that you can remember, but there are still many options. You could base your password on the initial letters of words in a favourite song or poem.

Changing your password

Your password will expire after 90 days and you will then have to change it. To change your password you will have to enter your old password and then enter your new password twice. This ensures there are no discrepancies when entering your new password.

Advice for Line Managers

Your staff should have the correct level of access to be able to carry out their duties.

You should ensure that staff have the correct level of access when transferring or commencing employment. You should also ensure that staff do not retain inappropriate access to information systems which are no longer required due to a change of role.

You should not condone the sharing of passwords.

Appendix C: Use of GMP Electronic Mail (E-mail)

Use of email, Sending emails outside European Economic Area, SPAM and hoax email

Use of email

Electronic mail or 'email' is a unique medium for communication. Messages received at your workstation can be replied to, or forwarded, very easily and can reach a wide audience. Care must be taken when using email as a means of communication as all expressions of fact, intention and opinion via email may bind you and/or GMP and can be produced in court in the same way as oral or written statements. The advantage of email is that it is an extremely easy and informal way of accessing and disseminating information. The same principles apply to information exchanged in this way as apply under the terms of your employment contract to any other means of communications. GMP does not tolerate any behaviour, action or language that could be perceived to be discriminatory or offensive to an individual or group. Any action that brings your professionalism and integrity into question will be dealt with through the appropriate disciplinary and possibly criminal processes. If you use email for purposes that are not related to your duties you may be asked to justify your actions.

Email is now the prime vehicle for communication across the Force and should be used in preference to paper transactions wherever possible. However, consideration should be given to the nature of the information being communicated as some subject matter will not be suitable for email, e.g. sensitive personnel information (medical, welfare, in-confidence) should not be sent by insecure means. The email system is suitable for documents up to and including the GPMS marking of 'RESTRICTED' for internal emails or emails routed securely via e.g. PNN, CJX addresses, but not emails sent to insecure email accounts e.g. sky.com, hotmail.com, anycompany.co.uk. GPMS marking should be applied to email in line with Force policy.

Sending emails outside European Economic Area

The Information Governance Manager, Information Services Branch, should be consulted prior to sending an email containing personal data, outside the European Economic Area (EEA) as additional safeguards should be followed.

SPAM and hoax email

There is an element that wishes to disrupt email systems by flooding them with hoax and spam email. GMP have invested heavily in trying to prevent spam from reaching your workstation but occasionally there may be one that gets to your mail box. You can either delete the email or forward the email to the Spam mail box. This is achieved by typing SPAM in the "To" address box. Hoax emails are those that promise untold rewards or dire consequences if the email is not sent to "everyone in your address book". The only action you should take on this type of email is to forward the email to Information Security. The majority of these types of emails are hoaxes. Under no circumstances should the email be forwarded to anyone outside of GMP. The addition of a GMP address will add to the authenticity of the email. Check before you send.

Appendix D: Use of Internet

Appropriate Internet Access

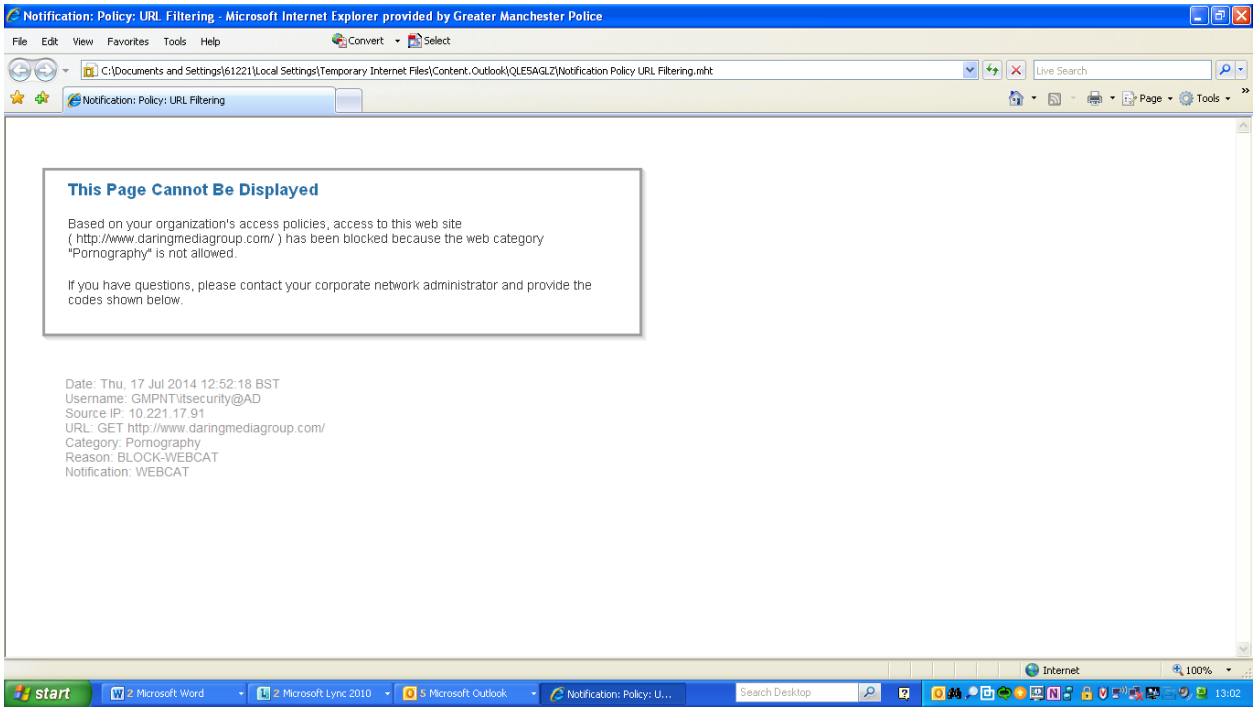
Appropriate Internet Access

GMP have invested heavily in providing a solution that manages access to the Internet. This is done via categories and the solution provider adds every Internet site into a relevant category. Although GMP has no control over which site goes into which category, it is possible to manage access to the categories.

The Professional Standards Branch, in conjunction with Information Security, have determined the categories that GMP personnel may access.

The following categories are not allowed by default but may be allowed for policing purposes: Adult, Advertisements, Child Porn, File Transfer Services, Filter Avoidance, Freeware and Shareware, Gambling, Games, Hacking, Instant Messaging, Internet Telephony, Lingerie and Swimsuits, Lottery and Sweepstakes, Online Storage and Backup, Online Trading, Peer File Transfer, Porn, Social Networking, Software Updates, Tasteless or Obscene, Web-based Chat.

If a site is blocked by the GMP solution you will receive notification that the category has been blocked. The example below shows a site that has been blocked because the category is Pornography.



If you need access to such sites you should contact the Information Services Branch Service Desk on 61400 and request that you be allowed access to the category that has been denied.

Appendix E: Social Network Sites

Security and Personal Risks, Unacceptable Content

Security and Personal Risks

Social networking sites have varying levels of security and, as public sites, all are vulnerable to unauthorised access attempts. GMP business is not to be discussed or referred to on social networking sites, even in private messages between site members who may be authorised to access your information. The only occasions where GMP business can be discussed on these sites is when it has previously been authorised through the Force Media and Social Media Communications Policy and Procedure.

Police Officers and Staff should be aware that social networking websites are a public forum and should not assume that entries on any website will remain private. Local and national media monitor social networks and will be looking for potential stories about GMP and its staff. You should be mindful of this and maintain the highest professional standards.

It is advised that you should use the appropriate privacy settings to ensure your profile is protected and not open to the general public. However, the terms and conditions on sites usually include waiving copyright, therefore anything you post could be used by the media or other parties. Identifying you work for GMP or have a connection to it may put you at risk. You could become a target, blackmailed or render yourself and your family to personal threats.

Unacceptable Content

Any inappropriate comments or images found on social networking sites will be investigated in accordance with Professional Standards of Behaviour for Police Officers, or Police Staff Standards of Professional Behaviour, which if proven may result in dismissal.

The investigation will consider whether the allegations bring GMP into disrepute by being one or more of the following examples, the list of which is not exhaustive:

- Defamatory
- Racist
- Sexist
- Homophobic
- Abuse re Religion or Religious Beliefs
- Obscene
- Indecent

Police staff should not compromise their position within GMP with their political or religious views but should maintain their impartiality and integrity.

Police regulations mandate that Police Officers are to carry out their duties with fairness and impartiality and in accordance with current legislation. They are not to discriminate unlawfully or unfairly. An officer's political beliefs should in no way compromise or affect their duties to the public or their decision making.

Appendix F: Use of GMP iPads

Overseas use, Use of wireless networks

Overseas use

The iPad user must carefully consider the risks of taking the device overseas. They need to consider how they can maintain physical security, especially if on holiday when the user is likely to be separated from the iPad for considerably longer periods of time than on a business trip.

Physical security provision in an hotel might be inadequate. A hotel room safe, or hotel reception secure storage is often not adequate to ensure that your device is not compromised.

The user must also consider the local regime of the country where they are visiting. This might be more of a risk entering China, Iraq or Russia than France or Spain. Whilst passing through customs the device may be removed and out of sight for a period of time and the device could be compromised upon it's return, or simply not returned.

Consideration should be given to:

- Leaving the device behind;
- Wiping the device prior to departure to ensure it holds no Force data;
- Wiping the device on return, after removing relevant Force data captured whilst away, to ensure the device is restored to a known secure state. This is especially relevant if the device has been out of sight at any time.

Use of wireless networks

Wireless networks provide high speed internet access but their use is not without risk. In common with all mobile devices, the iPad will always search for known wireless networks and try to connect to them.

Wireless networks are designed to be resilient and efficient, so to avoid contention with other wireless networks in the vicinity, will switch frequencies and power levels to provide the best service for any connected devices.

When connected, the network and device agree on a frequency with little interference and at as low a power level as possible to maintain communication. If the user moves locations, the power level may be raised to retain communication.

The iPad will 'call out' to the wireless networks that it has previously used until that wireless network responds. Each wireless network then listens for such calls, and the devices connect. However, it is possible to scan wireless networks, listening for devices calling for a wireless network that they know and then configure a network to appear to be the network that is called for. It will then appear to be the known network and the devices will connect. This is an attack on wireless devices known as 'The Evil Twin', and it is now written in applications available for current mobile hardware, such as Android phones.

An ‘Evil Twin’ attack can be used when the attacker can provide a stronger signal than the known, trusted network. It can thus work from a considerable distance, if the network is a home network and the user is away from home, or it may only work over a short distance in an internet café scenario. Any communication that is secured from the iPad all the way to its destination is unaffected by an ‘Evil Twin’ attack. This security is provided by the Good software.

However, any unsecured activity may be visible to an attacker. This would include native iPad email and internet browsing. Whilst the iPad is connected to an ‘Evil Twin’, it is possible for an attacker to launch other attacks on the iPad, however currently the risks appear to be based around observation of communication than on attacking data stored on the iPad.

The best practices for WiFi are therefore to switch wireless off (via the *Settings* option), unless it is needed. If WiFi is switched on, users should observe what network the device connects to, and ensure this makes sense, i.e. that it connects to the network you would expect. Users should consider how much they trust a network before using it, based on their physical location. In cases where users trust the physical security around their location as well as the network (e.g. home network at home or any Force HQ network) then the connection can be trusted. Conversely, a hotel network or a wireless café network, for example, should be much less trusted and users should carefully consider their use of the network in these circumstances.

Use of 3G networks will be slower but are more likely to be secure.