
The Leveson Inquiry into the Culture Practices and Ethics of the Press

Exhibit Ref: JK/5

Witness: ACC Jerry Kirkby

Date Produced: 21 March 2012

Description: Surrey Police Security Matters Handbook

Signature: 

Document Attached.

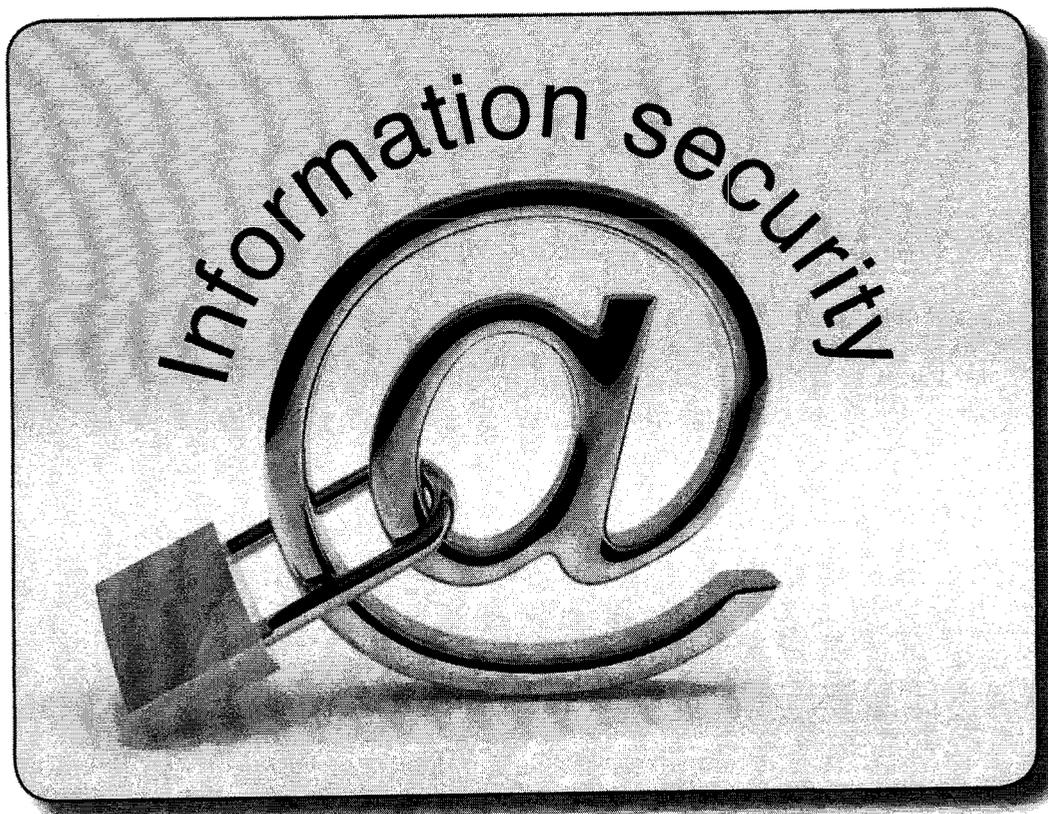
Surrey Police Security Matters

You have a role in protecting Surrey Police information and assets.

This handbook gives you advice and guidance on the main security issues that are likely to affect you as an employee of Surrey Police.

It also sets out your individual responsibilities.

If you require more information on any of the subjects within this handbook please go to the Policy and Procedure pages of the Surrey Police Intranet or email Information Security for advice.



NOT PROTECTIVELY MARKED

Contents

	Page
Computer Systems	<u>3</u>
Clear Desk	<u>4</u>
Clear Screen	<u>5</u>
Computer Viruses	<u>6</u>
Passwords	<u>7</u>
Email	<u>9</u>
Internet Access	<u>10</u>
Social Networking	<u>11</u>
Social Engineering	<u>12</u>
Government Protective Marking Scheme	<u>13</u>
Legislation	<u>17</u>
Physical Security	<u>18</u>
Laptops and other Portable Devices	<u>19</u>
Remote Working	<u>20</u>
Small Ads	<u>21</u>
Other Employment/Business Interests	<u>22</u>
ID Passes	<u>23</u>
Visitors	<u>24</u>
Changes in Your Circumstances	<u>25</u>
Drugs and Alcohol	<u>26</u>
Conflicts of Personal Interest	<u>27</u>
Gifts and Hospitality	<u>28</u>
Uniform and Equipment	<u>29</u>
Helpful Numbers	<u>30</u>

NOT PROTECTIVELY MARKED

NOT PROTECTIVELY MARKED

Computer Systems

Surrey Police information is held on a variety of computer systems.

Computer systems include computers, networks, Internet, Intranet, e-mail, telephony systems and also extends to mobile devices such as laptops, Personal Data Assistants, Mobile Telephones and removable media such as USB memory sticks, DVDs or compact disks, etc.

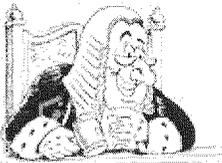
Your specific role will determine which computer systems you will need to access in order to perform your role effectively.

Some of the systems require additional log-on procedures whilst others do not.



It must be understood that whilst you may be able to access a system this does not give you the right to access that system at any time other than for legitimate reasons.

You must not disclose Surrey Police information to **any person** who does not have a legitimate reason to have that information.



If you access any information held on a computer without authority, or if you use a computer for a purpose for which you have no authority (for example **curiosity**) you are committing a criminal offence!

Surrey Police computer systems are provided for Police business use, however, limited personal use may be permitted, as defined in the supporting Use of Surrey Police Systems procedures, e.g. Use of Surrey Police E-mail System.

Surrey Police computer systems are monitored and audited.

Surrey Police **does not tolerate** inappropriate use of any of its systems. Any apparent breach of the computer systems policies will be investigated and where appropriate disciplinary action will be taken up to and including dismissal.

It is your responsibility as a user of Surrey Police computer systems to comply with the Acceptable Use of Surrey Police Computer Systems policies.

NOT PROTECTIVELY MARKED

NOT PROTECTIVELY MARKED

Clear Desk

To ensure the security and confidentiality of information, wherever possible, Surrey Police has adopted a clear desk procedure for papers and removable storage media and a clear screen procedure for information-processing facilities. This is to reduce the risk of unauthorised access, loss of, and damage to, information during and outside normal working hours or when areas are unattended.

Reduce the risk of inappropriate disclosure by only sharing official information, within the course of your duties, with those who are suitably security cleared, and who 'Need to Know' the information to carry out their work effectively.



At the end of each day or when not in use, information including printed paper, paper files and removable computer devices, i.e. CDs, disks, USB memory sticks and printouts should be stored in suitable, locked safes, cabinets or desk drawers – remember to make the key secure too

If cabinets and lockable drawers are not available, office doors should be locked when unattended.

Printed sensitive or protectively marked information (GPMS) should be cleared from printers, photocopiers and faxes immediately. Sensitive or protectively marked information, including copies, must be appropriately destroyed by shredding when no longer required.

Media should not be placed so it is visible to unauthorised persons through windows/doors.

If fitted, close the blinds at the end of the day.



Information left on desks is more likely to be damaged or destroyed in the event of a disaster such as fire, flood or explosion.

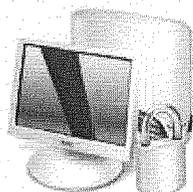
NOT PROTECTIVELY MARKED

NOT PROTECTIVELY MARKED

Clear Screen

If you leave your computer logged on when you are away from it, it may be possible for information held on the computer system to be read, printed or copied by someone not authorised to see it.

They could also change your documents or create new ones or send inappropriate emails – all of which would be your responsibility!



So, always lock your workstation
(by pressing **Ctrl, Alt, Delete**)
when leaving the room.

Ensure you **shut down**
your workstation at the
end of your working day.

Wherever possible, computer screens should be angled away from the view of unauthorised persons. If necessary, close the blinds if you have them.



Whilst Line Managers and Supervisors are responsible for ensuring their staff clearly understand and adhere to this procedure, it is your responsibility to help maintain the security and confidentiality of Surrey Police information.

NOT PROTECTIVELY MARKED

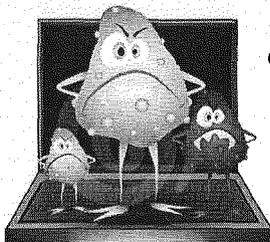
5

NOT PROTECTIVELY MARKED

Computer Viruses

All computers are vulnerable to malicious software (malware) attacks. Malware comes in the form of computer Virus, Worm or Trojan Horse. Using a computer network increases that vulnerability substantially.

A computer virus is a malicious computer program that can copy itself and infect a computer without your knowledge or permission.



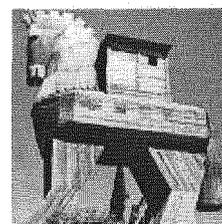
A virus can only spread from one computer to another when its host is taken to the uninfected computer, for example by a user sending it over a network or the Internet, or by carrying it on a floppy disk, CD, or USB memory stick.

Once the virus is on your computer it patiently waits to be 'triggered', by reaching a certain date or typing a particular sequence of keystrokes.

A virus can do things such as send email to everyone in your address book, make your computer run very slowly or wipe out all the data on your hard drive!

A worm can spread itself to other computers across a network but does not infect other files. Once a worm has copied itself to your computer it can scan your hard drive for information such as bank details, credit card numbers or passwords. The worm then emails the information back to the originator of the worm!

A Trojan Horse is a type of virus that attempts to make the user think that it is a beneficial, interesting or fun application. A Trojan Horse can allow a hacker to run hidden tasks or allow remote access to your computer by a third party. Symptoms of Trojan infection may include: destruction of data; Windows colour settings change; mouse function buttons reverse



Our Anti Virus software should detect any malicious software. However, if you think there maybe a virus on your computer, contact the **ICT Service Desk immediately on extension 2346** or by emailing **!ICT Service Desk**



If you send documents from home to your Surrey police email account or are intending to use data from a floppy disk, CD, or approved USB memory stick, you must make sure they are free from viruses before using or opening them by using the Sophos Anti Virus software on your workstation – double click on the shield on the bottom right hand side of the task bar

Where it is found that a virus or similar malicious code is received from a home account that "infects" the Surrey Police network or systems, you may be subject to disciplinary action.

NOT PROTECTIVELY MARKED

NOT PROTECTIVELY MARKED

Passwords

Access to Surrey Police computer systems (referred to as "log in" or "log on") is controlled by a username and password. The username identifies you as a valid user of the system and the password authenticates you as who you say you are and that you are authorised to use the system. Passwords that can reliably confirm your identity are crucial to the security of Surrey Police computer systems.

Always Use Strong Passwords

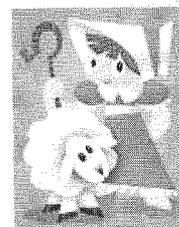
A strong password will have the following characteristics:

- Are at least **eight** alphanumeric characters long
- Contain both upper and lower case characters(e.g. a-z, A-Z)
- Contain numbers and punctuation as well as letters e.g. 0-9, < ! @ + ~ (%] \ | etc.
- Are not words in any language, slang, dialect or jargon.
- Are not something that is easy to work out with a little background knowledge. For example: personal information, favourite football team, birthday, pet or child's name
- Passwords should never be written down or stored online. Instead, try to create a password that is easily remembered, use the first letter of a memorable phrase or substitute letters for numbers.

For example;

Mary had a little lamb could become MaryH4daL1ttlelam8,

I stubbed my toe could become i\$tu88edmyT()e.



NOTE: do not use these examples as passwords!

Password Protection

Do not use the same password for more than one system, i.e., SPIKE, CIS, PNC, should each have an individual password. If you use the same password for every site, a hacker only has to break it once to have access to everything.

Do not share Surrey Police passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential Surrey Police information. If anyone, including ICT staff, demands a password, report them to Information Security immediately.

NOT PROTECTIVELY MARKED

7

NOT PROTECTIVELY MARKED

Password 'Don'ts':

- Do not use the "Remember Password" feature on any applications.
- Do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system (including Blackberries or similar devices) without encryption
- Do not reveal your password over the phone to ANYONE
- Do not reveal your password in an email message
- Do not reveal your password to your Supervisor or Line Manager
- Do not talk about your password in front of others
- Do not hint at the format of your password e.g. "my family name"
- Do not reveal passwords on questionnaires or security forms
- Do not reveal your password to colleagues to use while you are on holiday

NO ONE SHOULD KNOW YOUR PASSWORD EXCEPT YOU

If you think someone knows your password, change it immediately

Current Requirements for SPIKE Password Settings

Your password must be a minimum of **8** characters. Your password must be changed every **28** days. You cannot re-use your previous **12** passwords. Once you have changed your password you cannot re-change it for at least **2** days.

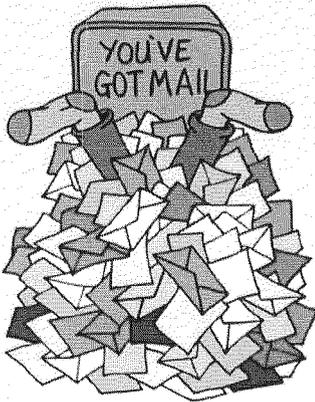


NOT PROTECTIVELY MARKED

Email

The use of email is an important, critical business function. It is also a high risk security area that, without proper safeguards in place, can leave the door open for intruders to access Surrey Police information.

Proper use of Surrey Police email is your responsibility.



Limited personal use - that is email that is not related to Surrey Police business or employment duties - is allowed provided that you comply with the terms of the Acceptable Use of Email Procedure

If you use the Surrey police email system you must have **no expectation of privacy.**

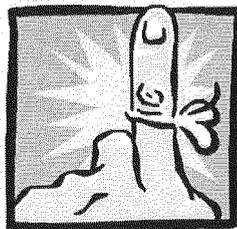
You must remember that **all messages** sent by e-mail from your workstation are owned by Surrey Police and Surrey Police reserves the right to access and disclose all messages sent over its e-mail system, for any purpose

You must:

- ❖ Not send emails or email attachments that contain obscene, profane, inflammatory, threatening, harassing (racially, sexually or otherwise), disruptive, or otherwise offensive language and including anything that will reflect poorly on the name or reputation of Surrey Police
- ❖ Not conduct trivial debates or chit chat with others
- ❖ Not send or forward chain emails or unsolicited email (SPAM)
- ❖ Not include unsuitable attachments such as video clips, images and executable files unless there is a genuine business reason to do so

If you receive unsolicited email (SPAM), report it to the ICT Service Desk (!ICT Service Desk). Do not click on any link, or attachment within the email and do not forward it to other people.

Did you know that email is a legally recognised document and as such can be used as part of a contractual agreement or obligation. Email can also be used as evidence in court.



Remember - You are personally responsible for the content of the email you send!

NOT PROTECTIVELY MARKED

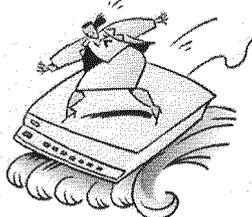
NOT PROTECTIVELY MARKED

Internet Access

You have access to the Internet via your SPIKE account and are permitted to use the internet for research purposes in accordance with your job role.
Personal use is restricted to recognised meal breaks.

Access to the Internet is restricted but should you require additional Internet access in order to carry out your work you must make your request via your manager and Professional Standards Department using the PSD Review form on the Intranet.

You are reminded that under no circumstances are you to attempt to access any site of an inappropriate nature except for authorised investigation purposes.
These **include** any site of a sexual, racist, sexist, or homophobic nature, or any site using inappropriate language.



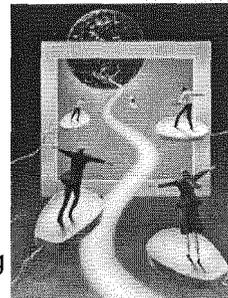
Under no circumstances may you download any games, video clips or Mpeg's. A similar restriction applies to documents from an unsolicited or unknown source, or which could cause offence to any member of the organisation.

The ability to access a site does not imply any approval of its content or sanction for private use during working time.

The Professional Standards Department monitors the use of the Internet by undertaking random audits.

Your manager can request reports detailing your activity if they suspect inappropriate use of web-browsing facilities.

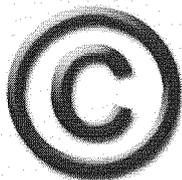
Downloading, uploading, posting, copying, possessing, processing and distributing material from the internet may be an infringement of copyright or of other intellectual property rights.



Courts have found organisations and their employees liable for infringement of copyright!

Copyright

The exclusive right to produce copies and to control an original literary, musical, or artistic work, granted by law for a specified number of years.



NOT PROTECTIVELY MARKED

10

NOT PROTECTIVELY MARKED

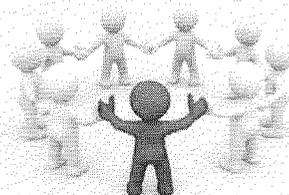
Social Networking

These guidelines are intended to assist you when considering your own personal use of social networking sites, both on and off duty.

It is strongly recommended that you do not identify yourself as a police officer or police staff on social networking sites unless a site is closed to the general public and the membership of the site is tightly controlled.

There have been instances of police employees placing themselves in difficult situations having disclosed their personal details on such sites.

If you create a site for the purpose of discussion with other police officers and police staff, or with members of the public, the site must clearly state that it is not an official Surrey Police site and does not represent the views of Surrey Police.



The site must not contain:

- ❖ offensive words or language in the title
- ❖ any content owned by Surrey Police, such as the Force Crest or other logos
- ❖ inappropriate entries, for example, racist or homophobic comments, disrespectful comments about Surrey Police as an organisation, foul language etc.

Should any inappropriate material be placed on a site that you own, it should be removed as soon as possible. Failure to do so may result in misconduct. If you are in any doubt, seek advice from the Professional Standards Department.

You may add comments or discuss police issues on such sites, providing there is no breach of confidentiality, no disclosure of operational information or no addition of comments that bring the force into disrepute.

Examples of breaches of confidentiality would include discussions of incidents.

Examples of disclosure of operational information would include surveillance tactics, crime investigation information or police staffing levels.



If you join an inappropriately titled site, having identified yourself as a police officer or member of staff, or join a site that contains inappropriate material, again having identified yourself as a police officer or member of staff, there is a potential misconduct.

As you can not guarantee who can access a site, even if a site is closed to the general public, there should be nothing within it that would compromise, embarrass or humiliate officers or staff if it were to be seen by others (including journalists). Neither should there be anything that could be considered to have brought the force into disrepute, or have the potential to do so. Images of staff naked or in intimate poses, would fall below an acceptable standard of behaviour, as would drunken, off duty behaviour.

Social Networking – Internet Sites Guidance

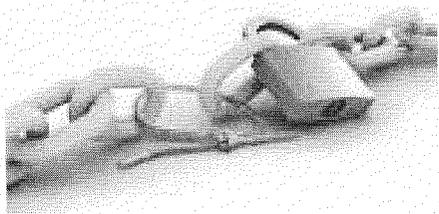
NOT PROTECTIVELY MARKED

11

NOT PROTECTIVELY MARKED

Social Engineering - Phishing

This is the practice of obtaining sensitive information by manipulating those who have legitimate access.



It is generally accepted that people are the 'weakest link' in security, and this is what makes phishing possible.

Social engineers exploit people's natural tendency to be helpful.

Telephone Security

Social engineers commonly use the telephone to trick people into revealing sensitive information.

When answering the phone do not immediately give out a lot of detail. Before giving out information;

- Verify the caller's identity
- Be satisfied they are legitimately entitled to any information requested
- Only disclose sensitive information on a '**Need to Know**' basis
- Always seek permission before giving out information about colleagues, including names, work locations, landline or mobile telephone numbers

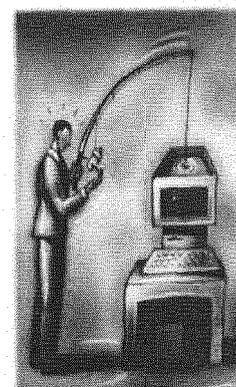
Security in Public Places

A common way for unauthorised persons to collect information about an organisation is by overhearing the public conversations of staff.

Do not discuss Surrey Police matters in places where your conversation may be overheard. You never know who might be listening.

If it is essential to discuss Surrey Police business whilst working in a public place, for example on a mobile phone, be discreet in what you say and conscious that you may be overheard.

*If you are approached and asked for information or asked to find out something by someone who should not be asking – **do not disclose any information** - report the matter to a line manager or the Professional Standards Department (PSD) as soon as practicable.*



NOT PROTECTIVELY MARKED

NOT PROTECTIVELY MARKED

Government Protective Marking Scheme (GPMS)

Surrey Police uses the Government Protective Marking Scheme which provides a common understanding across UK government and law enforcement agencies of the sensitive nature of documents and assets and the protection required in terms of handling, storage and disposal.

The deciding factor in assigning a particular level of marking is "what damage would be caused if the information fell into the wrong hands?"

Once the appropriate marking is assigned, GPMS helps you identify how to produce, send, handle, store and destroy protectively marked information.

Only people authorised to the level of the marking will be allowed access to a document, whilst also observing the "Need to Know" rules.

There are five levels of Protective marking:

CONFIDENTIAL PROTECT RESTRICTED
SECRET TOP SECRET

If none of the criteria for protective marking apply, then there is no need to protect it to these levels. Instead you should mark it as:

NOT PROTECTIVELY MARKED

All documents that require protective markings should be marked at the top and bottom of each page in **bold capitals** (via the header/footer facility), and each page should be numbered.

The majority of police information will be marked RESTRICTED, NOT PROTECTIVELY MARKED or PROTECT.

The small amount of SECRET and TOP SECRET information is generally only seen by ACPO ranks and Special Branch.

NOT PROTECTIVELY MARKED

NOT PROTECTIVELY MARKED

Examples of GPMS in the Workplace

NOT PROTECTIVELY MARKED

This would be the classification given to a schedule for an internal police training course. There is negligible risk if this information is compromised.

PROTECT

Protect is rarely used in the Police service as most documents are either 'Not Protectively Marked', 'Restricted' or 'Confidential'.

RESTRICTED

Professional Development Reviews (PDR) are marked restricted. PDRs contain information that is private.

CONFIDENTIAL

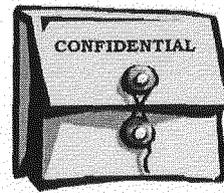
This classification would be used for an operational plan to police a demonstration against animal rights activists at an animal testing laboratory. This type of operational plan may contain information relating to company owners or employees.

NOT PROTECTIVELY MARKED

14

NOT PROTECTIVELY MARKED

Security of Protectively Marked Material



Storage

PROTECT and RESTRICTED	Lock away in a desk drawer or filing cabinet. Remember to keep the key safe!
CONFIDENTIAL	Storage must be in a locked filing cabinet within secure location, e.g. a locked office
SECRET and TOP SECRET	SECRET and TOP SECRET assets must be stored following consultation with Special Branch or Information Security

Disposal

	PROTECT & RESTRICTED	CONFIDENTIAL	SECRET & TOP SECRET
Disposal of paper assets	Dispose of to prevent reconstruction - Shred locally where available. Otherwise, place in secure waste bins or sacks for destruction (sacks must be secured pending collection)	Dispose of to prevent reconstruction - Shred locally in an approved crosscut shredder.	SECRET and TOP SECRET assets must be disposed of following consultation with Special Branch or Information Security
Disposal of magnetic media and optical media	Floppy disks – dismantle casing and shred disk CD ROM/DVD/Video/Audio Tapes/Hard Drives – require special disposal. Consult ICT or Information Security		



NOT PROTECTIVELY MARKED

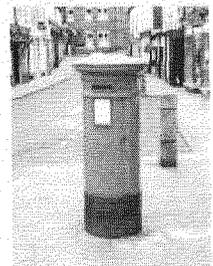
NOT PROTECTIVELY MARKED

Internal Post

- **RESTRICTED** assets in a new sealed envelope/package showing the protective marking on the outer cover
- **CONFIDENTIAL** assets in a new sealed envelope / package with protective marking shown
- Transit envelopes should only ever be used for **NOT PROTECTIVELY MARKED** assets

By Royal Mail Post or Courier

- **RESTRICTED** assets in a sealed envelope with no protective marking displayed
- **CONFIDENTIAL** in a double envelope package, both fully addressed with protective marking and a return address shown only on the inside envelope



By Email on Surrey Police Network and Criminal Justice Network

- **RESTRICTED** assets may be dispatched but must comply with Surrey Police email policy
- **CONFIDENTIAL** assets may not be dispatched without encryption

By Internet Email

- **RESTRICTED** assets may be dispatched but must comply with Surrey Police email policy
- **CONFIDENTIAL** assets may not be dispatched without encryption



NOT PROTECTIVELY MARKED

Legislation

Misuse of communications systems whilst at work is covered by **several** regulations, **some** of which are described below:

Official Secrets Act 1989

The Official Secrets Act is one of several Acts of Parliament that regulate the disclosure of information that could be damaging to the national interest.

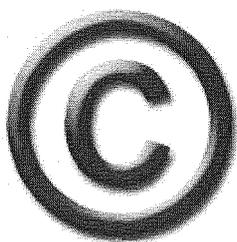
As the act is law you are bound by it whether or not you have signed it. Signing it is intended more as a reminder so you know you are under such obligations.



Computer Misuse Act 1990

This Act regulates accessing and/or modifying computer data without authority. If you access any information held on a computer without authority, or if you use a computer for a purpose for which you have no authority (for example **curiosity**), you are committing a criminal offence!

The Copyright, Designs and Patents Act 1988



This Act makes it a criminal offence to copy any software without the permission of the copyright owner. It is, therefore, illegal to make unauthorised copy of any licensed software or load unlicensed software onto your computer for whatever reason.

Do not *download* or *upload* music, games, videos, etc. to or from your workstation.

Data Protection Act 1998

This Act protects personal information, e.g. that which relates to identifiable, living individuals held on computers.

All public and private organisations are legally obliged to protect any personal information they hold.

Amongst other things it specifies that:

- Personal data must not be used or disclosed for reasons unrelated to the purpose for which the information was obtained
- Personal data must be accurate and kept up to date
- Appropriate security measures must be in place to protect against unauthorised access to, loss or destruction of personal data

If you breach any of the above Surrey Police could be liable to enforcement action by the Information Commissioner's Office.

NOT PROTECTIVELY MARKED

17

NOT PROTECTIVELY MARKED

Physical Security

Securing offices, rooms and facilities

You are responsible for keeping confidential any security measures, such as door access codes, to which you are entrusted.

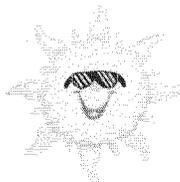
At the end of each working day ensure that all sensitive information and data is cleared away from desks and wall displays and secured in appropriate security cabinets or lockable drawers.

Paperwork must be removed from faxes and printers.



Make sure doors and windows are locked and alarms activated where fitted.

Do not assume that someone else will close the windows!



Doors must not be propped open – even during the hot weather.

Remember to **shut down** your workstation and **log off** your SPIRE telephone at the end of each working day.



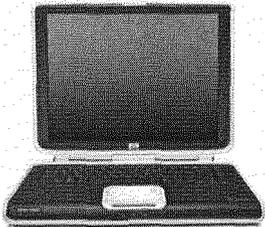
NOT PROTECTIVELY MARKED

NOT PROTECTIVELY MARKED

Laptops, USB Sticks, Mobile Phones and other Portable Devices

If you are issued with a laptop or other portable device, you are responsible for its security.

While laptop hard drives are encrypted to ensure information security, it is still vital that you report immediately to your line manager and ICT if your laptop or other portable device is lost or stolen.



It is essential that you do not keep your security password with your laptop.

Common sense and reasonable care must be used whilst transporting and using equipment away from the workplace

For example:

- keep your portable device in your sight on public transport and carry as hand luggage on flights
- during car journeys, keep your laptop in the boot out of sight and where practical remove it when leaving the vehicle unattended
- never leave your laptop or other portable device in your vehicle overnight
- use hotel safes/secure rooms if leaving equipment unattended
- avoid leaving equipment by windows or in the garden
- return your laptop to your workplace before holidays; do not leave your laptop at home when you are away

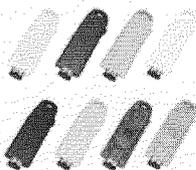


Unless your USB memory stick has been issued by the ICT Department, it must not be used on Surrey Police computers. Any attempts to use an unauthorised USB will be logged and regarded as a breach of the Force Information Security policy.

Unencrypted USB memory sticks pose several risks, including introduction of computer viruses, unauthorised removal of data and copying of applications.

Encrypted USB memory sticks may be obtained from the ICT Department, following your manager's approval.

An encrypted USB memory stick can be used to store protectively marked information up to and including CONFIDENTIAL level.



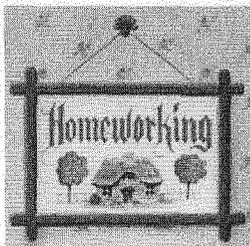
If you lose your memory stick you must inform ICT Service Desk immediately on ext 2346 or email ICT Service Desk.

NOT PROTECTIVELY MARKED

NOT PROTECTIVELY MARKED

Remote Working

Whenever you are working on Surrey Police business away from Surrey Police premises you are working remotely.



You should not send or forward police business-related e-mail documents or other police information to personal home e-mail accounts where unauthorised disclosure could harm the reputation of Surrey Police, could result in litigation against Surrey Police or is classed as "RESTRICTED" or above under the Government Protective Marking Scheme, unless there is evidence to support an operational imperative or need.

You should be aware that there are inherent risks when sending e-mails to your home computer and you are personally liable under the Data Protection Act 1998 in the event of this information being unlawfully obtained or disclosed to unauthorised individuals or organisations. For these reasons, the following guidelines should be adhered to:

- That only you and no other person in the household has access to your inbox account (that is no shared passwords or "family" Inboxes).
- Up-to-date anti virus software protection and, if available, a personal firewall is used on the user's home computer.

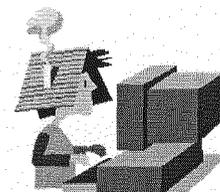
In addition, you should be aware and ensure that:

Any documents or emails should be deleted immediately after use or when returned to the user's force email account. They are not to be retained on their home e-mail account or computer hard drive for longer than is necessary.

You must check to ensure that any documents sent to your Surrey Police e-mail account from your home computer are free from viruses using the Sophos Anti-Virus software before opening them.

Where it is found that a virus or similar malicious code is received from a home account that "infects" the Surrey Police network or systems, you may be subject to disciplinary action.

Users are reminded that when force e-mails are sent to home e-mail accounts, the home e-mail account details may be stored by Surrey Police and that their home computer, peripheral devices or other removable data storage devices could be subject to seizure and forensic examination in the course of any investigation, where it is believed that relevant information may be held on that computer or devices to assist in that investigation.



NOT PROTECTIVELY MARKED

20

NOT PROTECTIVELY MARKED

Small Ads

'Small Ads' is a mailbox on MS Outlook that is used by Surrey Police employees to advertise goods for sale.

Small Ads must only to be used to advertise your privately owned goods for sale or property to buy/rent/let or to request wanted items

Small Ads must not be used to recommend, criticise or advertise other businesses, even if that business is owned or managed by a Surrey Police employee.



It is not permitted to include images of any kind on Small Ad items.

Nor is it allowed to include links to internet sites

Any items restricted by law, for example alcoholic beverages, tobacco goods or weapons are not to be advertised

The sale of football tickets is not allowed as under the Criminal Justice and Public Order Act it is a criminal offence for you to resell a spare ticket - even if it is for cost price or less. You can't even give it away!

The use of Small Ads to gain sponsorship for charitable work for example the London Marathon or fun runs, is permitted.

Links to charity websites are not permitted.



Surrey Police does not endorse or accept liability for any items placed on this mailbox.

Adverts must not contravene any part of the Use of Surrey Police Email System Procedure.

Any failure to observe these requirements will automatically result in the deletion of the Small Ad, without notification to the person posting the ad

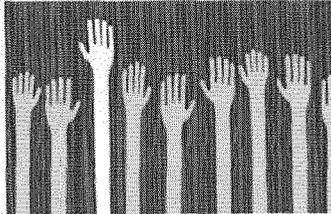
NOT PROTECTIVELY MARKED

21

NOT PROTECTIVELY MARKED

Other Employment / Business Interests

If you have another job, paid or voluntary, outside of the police service, you need to inform your line manager who will take an initial view as to whether this role is compatible with the interests of the police service.



If you are a police officer, you will also need to inform the Professional Standards Department to gain authorisation prior to carrying on any secondary employment or business interest.

You can do this via People Solutions which your line manager must also endorse to show that they are satisfied that there is no conflict of interest with your current role.

In deciding whether a second job or business interest will be allowed, the following criteria will be considered:

1. Number of hours worked
2. Impartiality
3. Impact on Surrey Police
4. Your current performance
5. Your health, safety and well-being.

Business Interest Policy – for Police Officers



NOT PROTECTIVELY MARKED

NOT PROTECTIVELY MARKED

ID-Access Cards

In the interests of security, identity cards **MUST** be worn, and clearly visible, at all times whilst on Surrey Police premises. Except for operational reasons they should not be worn off-site.

The main threat to security is from intruders by-passing our security system.

The threat is heightened if employees fail to wear their warrant or identity cards, or wear them in positions where they are difficult to see.



The following procedures apply whilst attending Surrey Police premises:

- ❖ All Police Officers, Special Constables and PCSOs in uniform must carry their Warrant cards
- ❖ All non-uniformed Police Officers must visibly display their Warrant card
- ❖ All other Police Staff must visibly display their identification cards prominently at all times
- ❖ Police Officers visiting from other Forces must visibly display their Force Warrant card
- ❖ All other visitors must wear a Visitor's pass issued at Reception or Front Office Counter
- ❖ At no time will an access card held by a member of Surrey Police staff or other non-employee be allowed to be passed or loaned to any other person to gain access to Surrey Police premises

All employees are empowered, and expected, to politely challenge persons on Surrey Police premises not displaying appropriate identification.



In the event of your access card being lost or stolen, it is your responsibility to notify the PSD Vetting Unit immediately so that the system can be updated to prevent any further access. You must also inform, in writing, your Divisional Commander or Departmental Head.

Any breach of this policy and procedure should be reported immediately to a supervisor or manager.

NOT PROTECTIVELY MARKED

23

NOT PROTECTIVELY MARKED

Visitors

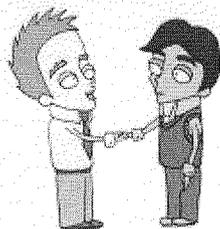
Visitors to Headquarters

(Visitors to Divisions must comply with local directions or instructions)

You should inform Reception of any visitors to HQ prior to arrival by either email, a Visitors form, or by telephone.

On Arrival

Reception will direct all visitors' vehicles to the Reception car park to park their vehicles.



All visitors must report to Reception where they will be greeted, signed in and asked to wait.

You will be informed of the visitor's arrival and must come to reception to escort your visitor to the designated meeting/work point.

Visitors who should be escorted **at all times** whilst on site will be given a red 'Escorted' lanyard.

All other visitors will be issued with a green 'Unescorted' lanyard.

If you see a visitor wearing a red 'Escorted' lanyard unescorted within secure areas, you are **encouraged to challenge** the visitor to ensure that he/she complies with this procedure.

Visitors will not be directed or given access from Reception. **You** are the person responsible for ensuring that the visitor complies with this procedure.

On Departure

All visitors must report to Reception to sign out and hand in their badge.

The 'Escorted' visitors must be escorted back to reception.

The Reception officer will then sign out the visitor on the register

Visitors From Other Forces

Must report to Reception and sign in as a visitor and must be met by their staff contact - ID Badges/Warrant Cards must be visible at all times.

Parking at Headquarters

All HQ personnel parking their vehicle on site must display their FIN or Collar number on their vehicle where it can be clearly seen.

Due to severe congestion in Police car parks, all visiting Surrey Police Personnel parking a vehicle on site must ensure a valid FIN/Collar number and phone number are clearly displayed so that they can be contacted quickly.

Disabled Parking

Only vehicles displaying a valid Disability badge are permitted to use the parking bays reserved for disabled drivers. Drivers of vehicles not displaying a badge will be required to immediately move the vehicle.



NOT PROTECTIVELY MARKED

NOT PROTECTIVELY MARKED

Changes in Your Circumstances

When you first join Surrey Police you have to go through a vetting process to gain a security clearance.

Your personal circumstances can, and often will, be subject to significant change over time and this may affect your suitability to maintain this security clearance.



It is, therefore, very important that you report any changes in your personal circumstances which may be relevant to your clearance, including spouses or partners, changes of address, change of co-residents, criminal offences or associations, financial circumstances or any other risk factor that could potentially impact upon your vetting clearance.



You can report relevant changes to the **Vetting** mailbox in the knowledge that notifications will be handled confidentially and met with a sympathetic response.

NOT PROTECTIVELY MARKED

NOT PROTECTIVELY MARKED

Drugs and Alcohol

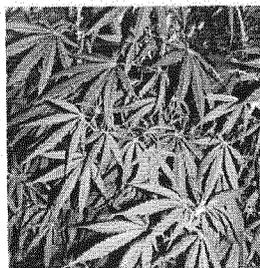
Surrey Police has a duty of care towards its employees and a desire to enhance public confidence in the service provided.

It is your responsibility to challenge any substance or alcohol misuse in the work place.

If you have reason to suspect a colleague may be suffering from a substance misuse problem, you should try to persuade that person to voluntarily seek specialist advice and the assistance of Occupational Health.

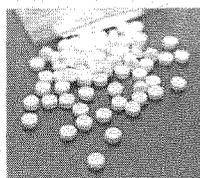
If they will not seek help then you must refer the matter to your line manager.

Similarly, if you believe you have a substance misuse problem, you have a clear personal responsibility to acknowledge your condition and seek assistance from the **Occupational Health Unit**.



The Force will provide support and treatment if you self declare a substance misuse problem. You will be expected to contribute to the cost of the treatment programme and you will be assessed on your ability to do so. If, however, you do not successfully complete the treatment programme you may be subject to disciplinary action.

Police Officers in safety critical roles such as Firearms officers or members or supervisors of Police Search Advisor (POLSA) Teams may be subject to regular substance testing. The force also has the power to test any officer if there is cause to suspect that the officer is misusing controlled substances.



If you need any further help, the Occupational Health Unit can provide advice and guidance on the effects of substance misuse and on referral services.

NOT PROTECTIVELY MARKED

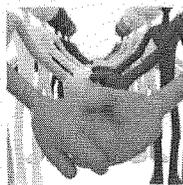
NOT PROTECTIVELY MARKED

Conflicts of Personal Interest

You are expected to declare any conflict of personal interest that could reasonably be perceived to have a detrimental impact on your ability to act in an objective manner.

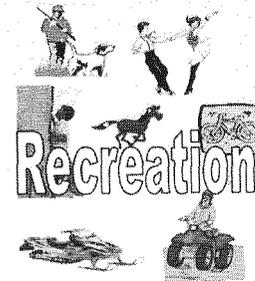
By declaring the interest this should protect you and the organisation from allegations of bias.

By 'personal interest' we generally mean: *'an out-of-work activity or relationship (past or present) between individuals that has the capacity to influence objectivity'*.



For example, a personal interest could range from a close personal friendship, where it may be difficult to participate in a process with impartiality, through to a situation where an intimate relationship is taking place.

The key issue is that the 'authority' or 'influence' could be exercised to the holder's advantage by incentive or sanction over the other party involved.



Examples of activities where conflicts could arise are: performance assessments, promotion/selection procedures, pay decisions, discipline/grievance procedures, procurement of external contracts and partnership work.

If you think this applies to you, you should declare the interest to your line manager as soon as you become aware of any conflict.

NOT PROTECTIVELY MARKED

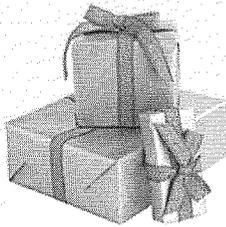
27

NOT PROTECTIVELY MARKED

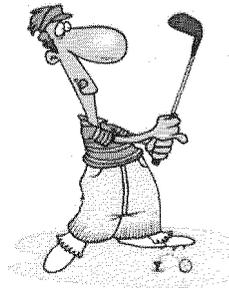
Gifts and Hospitality

Working for the police service puts you in a privileged position.

To use the authority of your position, particularly if you are a Police Officer, Special Constable or a member of Police Staff with designated powers, to obtain or gain a personal advantage is unethical and, in certain circumstances, a criminal offence.



You should never produce a warrant card or police staff identity pass, or wear whole or part uniform, to obtain discounts, goods or services unless as part of an approved arrangement.



However, you may come across circumstances where it might offend to refuse a gift or hospitality. Where this occurs you need to submit a hospitality, gifts and declaration of interest pro forma to the Head of Procurement who will provide you with guidance and advice.

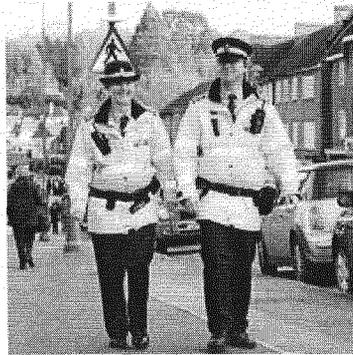
NOT PROTECTIVELY MARKED

NOT PROTECTIVELY MARKED

Uniform and Equipment

For the purposes of your role, you may be issued with uniform, operational equipment or a fuel card.

If you subsequently change your role, you should return any issued item you no longer require to your line manager.



If you decide to leave the force, it is your direct responsibility to ensure that whatever items are formally requested to be returned are returned to Surrey Police before you leave.

Security and safety considerations are paramount and the implications of these items being used by, or access being granted to, people other than those appointed by Surrey Police are significant.

It is for this reason that failure to return the property of Surrey Police may mean that you are charged for the current cost of replacing them.

A Uniform/Equipment return checklist can be found on the People Solutions application on the Surrey Police Intranet.



NOT PROTECTIVELY MARKED

NOT PROTECTIVELY MARKED

Email Contact Details

ICT Service Desk

!ICT Service Desk

Information Security

!Information Security

Data protection

!Data protection

Occupational Health

!Occupational Health Services

Vetting

!Vetting

NOT PROTECTIVELY MARKED

30