Surrey Police
Security Matters

Important Information:
Please read this document before your start date and bring it with you on your first day of employment with Surrey Police.

You are required to sign the Individual Declaration, found at the end of this document, when you accept your ID access pass.

~~~~~~

We are all responsible for ensuring we comply with Surrey Police Policies and Procedures.

This handbook provides advice and guidance on the main security issues that are likely to affect you in your day to day activities both at work and at home.

We must remember we are responsible for the protection of the public's information.

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.
~~~~~~

Contents

Continued…

Continued…

Security Summary

Do

- √ Wear your ID card at your place of work so it's easily seen
- √ Store printed information securely when away from your desk
- √ Change your password if you think someone else knows it
- √ If taking Surrey Police property i.e. laptops or information away from the office lock it in the boot of your vehicle before travelling and remember not to leave it in the vehicle overnight
- √ Always lock your computer screen if you are going away from your desk
- √ Politely challenge anyone not displaying an ID badge, tailgating or eavesdropping or shoulder surfing

Don't

- X Wear your ID card when you are in a public place
- X Share your password with anyone
- X Use anyone else's ID access card
- X Leave your ID card or mobile phone unattended on your desk or in your vehicle
- X Leave keys in locks, desk drawers, lockers and cabinets when away from your place of work
- X Leave workstations or laptops unattended without locking the screen
- X Allow anyone to use your computer account
- X Discuss police business in a public place or where you can be overheard

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 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 conducting checks on friends, relatives or celebrities… 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 Email System

Surrey Police computer systems are monitored and audited and you should legitimately expect the Professional Standards Department to be able to check all of the information systems, including Niche and the PNC in the course of their general duties as a part of ensuring professional standards are adhered to.

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.

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, 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, and photocopiers 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 window 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.

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 window 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.

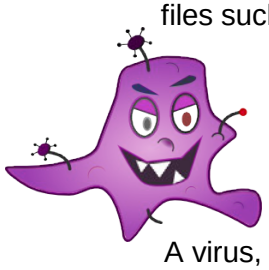
Remember to **shut down** your workstation and **log off** your SPIRE telephone at the end of each working day.

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 or by opening infected files such as .exe files or visiting corrupt websites.



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, may cause serious problems such as identity theft and fraud, or simply 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 may be a virus on your computer, contact the **IT Service Desk immediately** on **extension 33333** or via the **Shared Business Service Centre (SBSC) in People Solutions.**

If you send documents from home to your Surrey police email account or are intending to use data from a, 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 and click on 'Scan MY Computer'.
If you need to scan a disc or a USB click on 'Scans' and then 'Set Up a New Scan' and click the required box.

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

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 MaryH4daL1tt!elam8,

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, Niche, 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 IT staff, demands a password, inform !Information Security immediately.

Password 'Don'ts':

- Do not use dictionary words
- 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 Blackberrys 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 **90** days. You cannot re-use your previous **12** passwords.

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:

- 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 IT Service Desk on ext 33333 or via the Shared Business Service Centre (SBSC) in People Solutions.

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!

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, before or after duties.

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 line manager to the !Information Security mailbox or to the IT Service Desk via People Solutions.

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, or 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 Internet 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.

Social Networking

These guidelines are intended to assist you when considering your own personal use of social networking sites.

It is strongly recommended that you do not identify yourself as a police officer or police staff on social networking sites even if 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 have no reference to Surrey Police.

The site should 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 proceedings.

If you are in any doubt, seek advice from the Professional Standards Department.

You are strongly advised against discussing police issues on such sites. Be careful to avoid breach of confidentiality, disclosure of operational information or addition of comments that may 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 a site and identify 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, you may leave yourself vulnerable to disciplinary action.

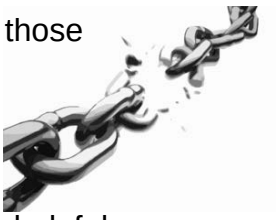
As you cannot guarantee who can access a site, even if a site is closed to the general public, there should be nothing within it that would compromise, embarrass or humiliate officers or staff if it were to be seen by others (including journalists).

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

For more information click on the link: Acceptable Use of Social networking Sites

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, call them back
- 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 for example the staff canteen or on the mini bus. You never know who might be listening. Your conversations may result in a breach of security.

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.*

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:

PROTECT **RESTRICTED**
CONFIDENTIAL **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.

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.

! **Mobile phones and Blackberries** should only be used for communications relating to information with GPMS classification up to **RESTRICTED**.

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	CD ROM/DVD/Video/Audio Tapes/Hard Drives – require special disposal. Consult IT or Information Security		

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

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 Parliamen

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 conducting checks on friends, relatives or celebrities…
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 unless expressly authorised for operational purposes.

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.

Officers and staff are liable to formal action, including arrest, if this Act is breached, for example disclosure from Niche or PNC.

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.

All employees are empowered, and expected, to **politely challenge** any person on Surrey Police/Shared premises not displaying appropriate identification.

.

Bear in mind access through doors and gates, ensure you see them close. Tailgating is a method that is used by some terrorists to test security responses, prior to an incident taking place.

Always use your ID Access card to gain entry to the site and remember, no tailgating.

Laptops, USB Sticks, Mobile Phones & other Portable Devices

If you are issued with a laptop or other portable device,
e.g. Blackberry, USB memory stick, VPN card,
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 IT if your laptop or other portable device is lost or stolen.

It is essential that you do not keep your security password or log-in procedures with your device. 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
- always lock your mobile device in the boot of your car before starting your journey, making sure it's not visible from outside and where practical remove it when leaving the vehicle unattended
- never leave your laptop or other portable device unattended in a public place such as dining rooms, meeting rooms or toilets and never leave it 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 IT 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 IT Department, following your manager's approval. All data must be deleted from the USB as soon as possible after use.

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

If you lose your portable device you must inform IT Service Desk immediately on ext 33333 or via the Shared Business Service Centre (SBSC) in People Solutions and complete the Loss of Handheld Device Reporting Form

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,
- 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 and in which case a line manager should be consulted.

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 (see page 8 for details).

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.

Small Ads

'Small Ads' 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 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 advert.

Other Employment / Business Interests

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

You can do this using the Business Interest Application Form 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 Guidance

ID-Access and Contractors

Access cards are used to ensure that only authorised people can access Surrey Police buildings. In the interests of security, identity cards **MUST** be worn, and clearly visible, at all times whilst on Surrey Police premises.

If you forget your card you must sign-in as a visitor.

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.

Except for operational reasons ID cards should not be worn off-site.

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

A lost card costs just a few pounds to replace but in the wrong hands our ID-Access cards are priceless!

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 Line Manager or Departmental Head.

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

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

Visitors and Contractors

Visitors to Headquarters

(Visitors to Police stations and other police offices 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

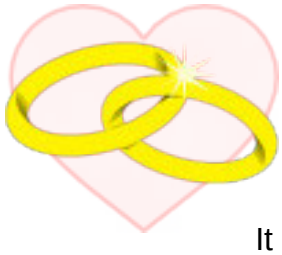
All HQ personnel parking their vehicle on site must display their FIN or Collar number on their vehicle where it can be clearly seen.
Due to severe congestion in Police car parks, all visiting Surrey Police Personnel parking a vehicle on site must ensure a valid FIN/Collar number and phone number are 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.

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.

New Home

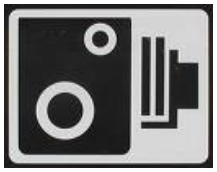
You can report relevant changes to the **!Vetting** mailbox in the knowledge that notifications will be handled confidentially and met with a sympathetic response.

Notification of Court Proceedings

You must report to the Professional Standards Department (PSD), via your Line manager / Departmental Head, if you are subject to any of the following:

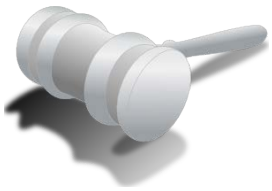
- Involvement in criminal proceedings either in the United Kingdom or abroad
- If you are the subject of a criminal investigation, irrespective of the outcome
- Any traffic offences where the individual is summoned or receives a Fixed Penalty Notice (FPN - Endorsable Only)
- Any dealings under the Penalty Notice Disorder Scheme, introduced by the Criminal Justice and Police Act 2001
- If you are the subject of an Anti-Social Behaviour Order
- If you receive a warning in the first instance under the Protection from Harassment Act 1997

The above applies whether you are on or off duty.



Reporting the Facts

The full circumstances of the incident must be submitted without delay to your Line Manger, who will forward it to the Professional Standards Department for recording and obtaining a proportionate decision as to the appropriate course of action.



Testimonials

Before you appear at any criminal or civil court, or any other type of formal tribunal in order to give testimony or character evidence, you must obtain written authority from the Head of PSD or, in their absence, a Detective Inspector of PSD. The intention is to reinforce the requirement that the actions of Surrey Police staff should not bring into question their impartiality.

You must make it clear to the Court that you are assisting in a private capacity, and are not representing Surrey Police.

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.

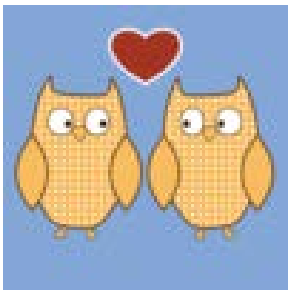
If you need any further help, the Occupational Health Unit can provide advice and guidance on the effects of substance misuse and on referral services.

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'*.



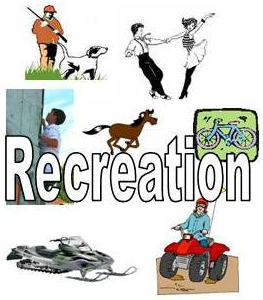
For example, a personal interest could range from a close personal friendship, where it may be difficult to participate in a process with impartiality, through to a situation where an intimate relationship is taking place.

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.



Declaring Associations

A key threat to the police service in terms of corruption is that of criminal association leading to the disclosure of intelligence, operational compromise and loss of public confidence.

You must report to **!Vetting** any non-work related association where you know or strongly suspect that the association is with a person who falls into the following categories:

- Persons known to be charged with a criminal offence and is the subject of a current prosecution.
- Persons known to be under investigation but not yet charged with a criminal offence.
- Private investigators or legal employees who due to their work and the association may leave the office/staff member vulnerable, for example, being asked to or at risk of sharing information or police methodology .
- Association with any group, organisation or society that could give rise to conflict of interest or the perception of bias in carrying out his or her work for Surrey Police impartially.

At no time should you conduct checks on PNC or Niche, or conduct any other enquiry, to gain information about relatives, friends or associates.

If it is suspected that relatives, friends or associates may fall within the area of this guidance, the information should be passed to the Professional Standards Department, Vetting Team without any checks being conducted.

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.

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 are due to leave the organisation, it is your direct responsibility to ensure that all items of uniform and equipment are returned to Surrey Police before you leave.

A Uniform and Equipment Return Guide can be found in the Knowledge Base in People Solutions:

People Solutions

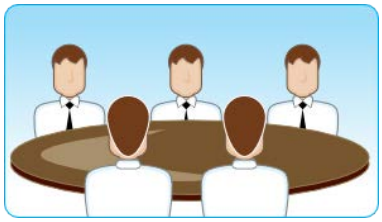
Security and safety considerations are paramount and the implications of these items being used by, or access being granted to, people other than those appointed by Surrey Police are significant.

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.

Removing Protectively Marked Documents from Police Premises

On occasions you may be required to remove documents from police premises and keep them with you at home. This should only be done when there is a business need, and should be approved by your Line Manager or Department Head.



For example;

- If you are attending a meeting near to the end of the working day and do not intend to return to your office
- If you will be attending a meeting the following working day and travelling to work to collect documents/information would be impractical

You should only take with you the information you specifically require and it must not be disclosed to, or be able to be accessed by, any third party.

You should travel direct from your place of work to your home address, where the information must be stored in an appropriate manner.

Police information must not be left unattended in vehicles.

Printouts from PNC and Niche (and similar) must not be taken off police premises unless there is an absolute necessity to do so.

If only specific parts of a document are required to view it may be necessary to remove or black out (redact) any personal, sensitive or irrelevant information that is not required before sharing or copying the document.

If you lose any police information, accidentally or through a criminal act (Theft of/from Motor Vehicle or Burglary etc.) you must report it as soon as possible to both the force where the loss occurred, and to Surrey Police via the Contact Centre.

If you are away attending a meeting all Police information must be securely stored when the meeting room is vacant, and it must not be left on tables or in areas where unauthorised third parties could accidentally gain access to it. If possible you should keep possession of any police information whilst at the event.

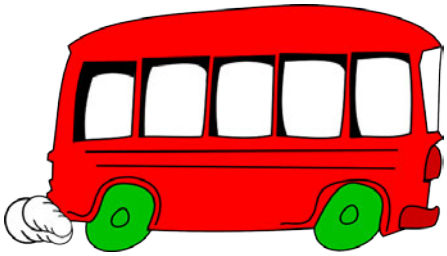
Your home computer must not be used for working on a protectively marked document. If a computer is to be used for such material, it must be authorised, issued and approved by IT.

This subject is extremely important, for more detailed information please read;

Removing Protectively Marked Documents from Police Premises

Travelling on the Surrey Police Courtesy Bus

If you travel on the Surrey Police courtesy bus at any time of day you must ensure you don not discuss any operational or sensitive information. Surrey Police officers and staff do not all share the same level of Vetting and may overhear conversations that should be restricted.



Also remember, there are occasions when members of the public travel on the bus and should not be exposed to sensitive or restricted police information.

Also known as ‘Social Engineering’, phishing is the practice of obtaining sensitive information by manipulating those who have legitimate access.

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

It’s therefore important not to discuss sensitive or operational matters in places where your conversation may be overheard – for example when talking on a mobile phone. Be discreet in what you say – you never know who might be listening.

Anonymous

Anonymous is an internal anonymous contact system that has been introduced to enable all officers and staff to report dishonest, corrupt, unethical, bullying, harassment or other inappropriate behavior.

The system facilitates a two-way communication between PSD´s Intelligence Team and any system user within the Organisation whilst maintaining the user's anonymity.

The PSD Intelligence Team has no way of identifying the user or the computer the report has come from.

All Surrey Police employees are responsible for ensuring that the Surrey Police Values are upheld. Any employee who is dishonest, corrupt or unethical compromises our high standards and potentially damages public confidence in the Force.

Any employee who knows about or suspects such behaviour and does nothing effectively condones it.

How to use the system

Simply type the word anonymous into URL line on Connect and press return

You will then be able to type in your report and you will be given a unique ID and you will be required to set up a password

The PSD Intelligence Team log onto the website and read the report. They acknowledge the report and if necessary ask for more information

Using your unique ID and password you can log on at any time to check on the status of your report and respond to any messages left by the PSD Intelligence Team

There is no obligation to log in again, nor reply to any question posed by the team

If you do not reply within 28 days of the last PSD Intelligence team response they will assume you do not wish to continue communication or provide further information

Alternative ways of reporting concerns

There are a number of other ways that you can report your concerns in confidence:

- Directly through your line manager
- Via a confidential email to !PSD Intelligence
- Crimestoppers 0800 555 111
- Independent Police Complaints Commission (IPCC) 08453 002 002

Useful Contact Details

IT Service Desk	.....	**Shared Business Service Centre**
Information Security	.....	**!Information Security**
Data protection	.....	**!Data Protection**
Occupational Health	.....	**!Occupational Health Services**
Vetting	.....	**!Vetting**
People Solutions	.....	**People Solutions**

Individual Declaration

I have read and understood the Security Matters document and agree to comply with my individual responsibilities set out in this document.

I understand my obligations with regard to the use of Surrey Police computer systems, access to email and the Internet and the use of Surrey Police telephony.

I acknowledge that failure to comply may result in disciplinary action.

During the course of my service, I may be issued with operational equipment, a fuel card or uniform. I will return these items when I leave the force.
I will also return my ID pass when required to do so.

SURREY POLICE
With you, making Surrey safer

Signature: ……

Print Full Name: ……

FIN Number: ……

Date: ……

It is your responsibility to ensure that you are aware of any changes.

This document is available on the Surrey Police Intranet