Surrey and Sussex Police
Secruity Matters

We are all responsbile for ensuring we comply with Surrey and Sussex 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 Joint Intranet or email Information Security for advice.

Contents

Security Summary

Do

- ✓ Wear your ID card at your place of work so it's easily seen.
- ✓ Change your password if you think someone else knows it.
- ✓ If taking Surrey and Sussex 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 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.
- ✓ Store printed information securely when away from your desk.

Don't

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

Computer Systems

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

This includes networks, Internet, Intranet, e-mail, telephone systems and also extends to mobile devices such as laptops, Mobile Data Terminals (MDTs), smart phones and removable media such as USB memory sticks, DVDs etc.

Your specific role will determine which computer systems you will need to access to perform your role effectively, some of which will require additional log-on procedures.

Please note that whilst you may be able to access a system, you only have the right to do so for a legitimate reason related to your job role.

You must not disclose Surrey and Sussex Police information to **anyone** 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 and Sussex Police computer systems are provided for Police business use, however, limited personal use may be permitted. This is defined in the supporting Surrey and Sussex Police Systems procedures, e.g. Use of Email Procedure.

Surrey and Sussex Police computer systems are monitored and audited. The Professional Standards Department can check the force's information systems in the course of their general duties to ensure professional standards are being adhered to.

Surrey and Sussex Police **do not tolerate** inappropriate use of any of their 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 and Sussex Police computer systems to comply with the Force Information Security Policy.

Computer Viruses

All computers are vulnerable to malicious software (malware) attacks. Malware comes in many forms such as Ransomware, Viruses, Worms and Trojan Horses. Using a network and connecting to the internet increases that vulnerability substantially.

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 01273 635145 or via the Self Service Portal on the intranet.

If you send documents from home to your Surrey Police email account or are intending to use data from a DVD, or **approved** USB memory stick, you must make sure they are free from viruses before using or opening them.

Clear Desk

To ensure the security and confidentiality of information, wherever possible, Surrey and Sussex Police has adopted a clear desk procedure for papers and removable storage media, as well as 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 of normal working hours or when areas are unattended.

If the need arises for photographs to be taken within Police premises, care should be taken to ensure that no sensitive policing material or personal data is visible in the photograph. When there is a policing need to display posters or briefing material on walls or notice boards, it is the responsibility of all staff to ensure it is taken down and disposed of in line with its handling instructions when it is no longer relevant.

At the end of each day or when not in use, information including printed paper, paper files and removable storage devices, i.e. DVDs, 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.

Sensitive or security classified information should be cleared from printers and photocopiers immediately. This information, including copies, must be appropriately destroyed by shredding when no longer required.

Information 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.

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, create new ones or send inappropriate emails – all of which would be your responsibility!

So, always lock your workstation (by pressing the **Windows** and **L** keys together) when leaving the room.

Ensure you log off and **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 and Sussex Police information.

Passwords

Access to Surrey and Sussex 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 while 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 and Sussex Police computer systems.

Always Use Strong Passwords

A strong password will have the following characteristics:

- It is at least **nine** characters long.
- It does not contain common words such as password, Surrey, Sussex, police, etc.
- It is not something that is easy to guess with a little background knowledge, for example: personal information, favourite sports team, birthday, child’s name.

We recommend using the NCSC’s **three random words** approach for creating a strong password. Simply choose three (or more) words that are memorable, but not easy to guess, and link them together – for example, VanityFrictionOpponent or EthicsSageSpring. You will meet the minimum 9 characters without even trying.

Note: don’t use these example passwords!

Password Protection

Re-using your password for multiple websites and systems is a big security risk. If your password is stolen, then the attacker may have access to everything. Therefore, you must not use the same password for more than one system, i.e., SURPOL/INT, Niche, PNC, must each have a different password.

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

Passwords should never be written down; you can store them on your computer as long as they are securely encrypted.

Two Factor Authentication (2FA) should be enabled whenever the option is available. This could be a code that's sent to you by text message, or that's created by an app, so even if an attacker has your password, they still won't be able to log in.

NO ONE SHOULD KNOW YOUR PASSWORD EXCEPT YOU

Never reveal your password to anyone under any circumstances.
If you think someone knows your password, change it immediately.

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 and Sussex Police information.

Proper use of Surrey and Sussex Police email is your responsibility.

Limited personal use (emails that are unrelated to Surrey and Sussex Police business or employment duties) is allowed provided that you comply with the terms of the Use of Email Procedure.

If you use the Surrey and Sussex Police email system you must have **no expectation of privacy**. You must remember that all messages sent by email from your workstation are owned by Surrey and Sussex Police and reserve the right to access and disclose all messages sent over its email 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 and Sussex Police.
- Conduct trivial debates or chit chat with others.
- Send or forward chain emails or unsolicited email (SPAM).
- 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 as SPAM using the Phishing button in Outlook (available with 365). If you don't have 365, forward it directly to !Phishing.

Do not click on any link, or attachment within the email and do not forward it to other people.

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

Remember - You are personally responsible for the contents of the email you send and who it is sent to, so ensure you are sending it to the correct person.

Internet Access

You have access to the Internet via your force 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 to the IT Service Desk Desk on **ext. 84444** or via the Self Service Portal on the intranet, providing line manager approval.

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 image files, 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.

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

Downloading, uploading, posting, copying, possessing, processing, or distributing material from the Internet may be an infringement of copyright or of other intellectual property rights which Courts have found organisations and their employees liable for.

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 or Sussex Police.

The site should not contain:

- Offensive words or language in the title
- Any content owned by Surrey or Sussex Police, such as the Force Crest or other logos
- Inappropriate entries, for example, racist or homophobic comments, disrespectful comments about Surrey or Sussex Police as an organisation, foul language etc.
- Any force data or private/sensitive information

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 forces 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, 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.

Resources

Social Media Policy

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 or contact numbers and **never** disclose personal contact information.

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 and Sussex Police matters in places where your conversation may be overheard for example the staff canteen or on the minibus.

You never know who might be listening. Your conversations may result in a breach of security.

If it is essential to discuss Surrey and Sussex 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.

When working from a force device in a public location always be mindful of who can view your screen and try to work in as private an area as possible where you cannot be overlooked.

*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 to the Professional Standards Department (PSD) and Security and Information Assurance/Information Security as soon as practicable.*

Resources

Information Security - information_security@surrey.police.uk

PSD Surrey - PSD@surrey.police.uk

PSD Sussex - PSD.Main@sussex.police.uk

Government Security Classification (GSC)

In order to appropriately store, handle, share and dispose of all information that is processed by Surrey and Sussex Police, security classifications must be applied to ensure the appropriate degree of protection.

Government Security Classification (GSC) has been designed to indicate the level of sensitivity of information, thereby helping to manage risk. Within GSC, information is marked under one of the following three categories:

- OFFICIAL
- SECRET
- TOP SECRET

Most information processed day to day within Surrey and Sussex Police will be OFFICIAL. All information that is not protectively marked as SECRET or TOP SECRET will automatically be categorised as OFFICIAL.

Marking Information

All Police information is considered to be OFFICIAL by default, and as such there is no requirement to routinely mark information as OFFICIAL. However, it may be necessary in certain circumstances.

For example, a document may be protectively marked as OFFICIAL if it is being sent outside of the organisation to a recipient who does not routinely handle Police information. This marking can reinforce certain principles, such as “need to know” or “do not disseminate”.

Some information may be of higher sensitivity but does not warrant the marking of SECRET. In these instances, the information should be protectively marked as OFFICIAL, with the *handling caveat* of:

- OFFICIAL - SENSITIVE

The OFFICIAL - SENSITIVE caveat allows information to be managed on OFFICIAL systems and networks, but implements additional safeguards to how it is processed.

Examples of where the OFFICIAL - SENSITIVE handling caveat should be used include:

- Corporate or operational information that an attacker could use to identify physical, procedural or technical vulnerabilities
- Commercial or market information which if leaked may result in reputational damage
- Personal information where compromise would directly threaten someone’s safety
- Information about investigations and civil or criminal proceedings that could compromise public protection or enforcement activities, or prejudice court cases
- Information about operations or covert assets or equipment that could damage capabilities or effectiveness

All documents that require a security classification 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.

Security of Government Security Classified Material

Classification	OFFICIAL	OFFICIAL - SENSITIVE
General	• Data must be stored and managed securely within Police approved systems. • Information should not be accessed, read or discussed where you can be overlooked or overheard. • Information should be protected by a governance suite including clear desk/clear screen and access control procedures. • Information may be removed from Force premises provided appropriate safeguards are in place to prevent material being lost or stolen. This must be accompanied by authorisation if significant volumes of material are to be moved. • Handling instructions from the sender/author must always be followed.	In addition to OFFICIAL: • Material must not be left unattended and should be locked away when not in use. • Information should only be communicated or passed to others on a need-to-know basis. • Information should not be read or worked on in sight of unauthorised persons and appropriate safeguards must be in place to prevent material being lost or stolen.
Storage	• Storage must be in a locked filing cabinet within secure location, e.g. a locked office. • Keys must be stored securely and accessible to only those authorised to use them. • Laptops must be locked away or secured in docking stations when left in the office, only encrypted laptops may be taken outside of a Police establishment.	
Email	• Information may be sent by secure email if available (i.e. those containing .pnn, .gcsx, .cjsm, .nhs, .gsi, etc.) • Information may be sent to a non-secure email address when appropriate, but steps should be taken to ensure recipients understand any restrictions on further circulation.	In addition to OFFICIAL: • Information may be sent to non-secure email addresses only on an exceptional basis if there is a pressing business need and no viable alternative, provided this is authorised and there is confidence that the recipient will follow any instructions on what can and can't be done with the information.

	• Sensitive or personal data should not be sent without encryption and / or the consent of the person who is the subject of the data.	
Post	• Information may be sent by normal post in a single, unused envelope. • Sensitive personal data must be double enveloped and either sent by courier/recorded delivery, or on encrypted removable media. • Seek permission from the Information Asset Owner for significant volumes of information	In addition to OFFICIAL: • Include return address on back of the envelope. • Never mark the classification on the outer envelope, but do mark it on an inner envelope. • Trusted hand under single cover for physical movement.
Removable Media	• Use of removable media should be reduced to the minimum level required to support the business. • Encryption should always be considered, and where required, should be government-grade.	In addition to OFFICIAL: • Government-grade encryption should always be used.
Telephone	• Telephones are inherently insecure, but can be used for conversations classified as OFFICIAL if care is taken to avoid being overheard. • Sensitive information should not be discussed by telephone, except where the operational value of having the discussion outweighs the risk.	
Printing	• Permitted unless handling instructions dictate otherwise. • Only ever print what you need. • Control copies appropriately	
Disposal	• Information already in the public domain can be disposed of in recycling or general waste. • Information should be disposed of securely according to internal policy and procedure.	

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 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 copies 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.

UK Data Protection Act 2018

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 loss, destruction or unauthorised access of personal data.

If you breach any of the above Surrey and Sussex 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.

General Data Protection Regulation – GDPR

The **GDPR** gives people more rights over their own data and expands the definition of personal data.

No matter what your role, as a Surrey or Sussex Police employee you are responsible for the data you handle. The public trust us to look after their information and prevent it from being misused or falling into the wrong hands.

Personally **I**dentifiable **I**nformation (**PII**) is any data that can be used to identify a living person. This consists of a person's: **name, address, phone number, email address, photograph or video recording, location data, or IP address.**

Examples of personal data breaches include:

- Access by an unauthorised third party
- Deliberate or accidental action (or inaction) by a controller or processor
- Sending personal data to an incorrect recipient
- Computing devices containing personal data being lost or stolen
- Alteration of personal data without permission
- Loss of availability of personal data

You must ensure you are protecting the information correctly and only share PII for policing purposes.

If there is a security breach involving PII, you must inform the Data Protection Officer **as soon as possible**, as certain information breaches must be reported to the Information Commissioner's Office (ICO) - within **72 hours** of the incident occurring.

Reports of this nature can be made using the **Security and Breach Reporting Form (SABR),** available on the Intranet.

Physical Security

Certain threat actors, such as opportunistic criminals, social engineers, malicious insiders or even terrorists will look to exploit potential vulnerabilities in physical security.

This could be through doors and windows left open or unlocked which provide access or a route to sensitive information or critical operational assets.

Perimeter Security

Security is everyone's responsibility. All officers and staff are encouraged to report potential security vulnerabilities in the perimeter, such as a damaged fence or a gate, insufficient security lighting or CCTV coverage, or lack of appropriate access control.

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

Tailgating is a very common method used by threat actors to test security responses, relying on employee's kindness and goodwill to allow them access. Make sure barriers, gates and doors close behind you when entering a site or premises. If you do not recognise the person behind you, ask to see their ID card.

Building Security

Most buildings on Surrey and Sussex Police will allow access through the use of an ID/Access card. If you lose this card, make sure it is reported immediately using the SABR form so that the access rights on the card can be blocked.

If the building you work in uses a digi-lock in order to access (whether this be an office door or a storage cupboard), it is your responsibility to keep that access code confidential. Do not write it down where it can be easily seen, such as on a white board in the office. When a member of staff leaves your team, or if you believe the code has been compromised, report to Estates and Facilities to get the code changed as soon as possible.

When you are the last one out of the office at the end of the day, conduct a thorough check of the building to make sure all windows are closed and locked. If your department has a security alarm, make sure this is set.

Depending on the building that you are working in, it may be difficult to control the temperature of your office, especially during hot weather. Doors should not be left propped open when the office is unattended.

Office Security

All officers and staff are reminded of the importance of the clear desk policy. At the end of each working day, it is your responsibility to ensure that all sensitive information and data is cleared away from desks and stored securely.

Check that no paperwork has been left in printers. If so, make sure this is stored or disposed of properly.

Laptops, USB Sticks, Mobile Phones & other Portable Devices

If you are issued with a laptop or other portable device, e.g. MDT, USB memory stick, VPN card - **you** are responsible for its security.

Laptops and hard drives are encrypted using BitLocker technology. However, 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 credentials 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, including going abroad
- Always lock your laptop 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

Only explicitly authorised USB devices will be permitted for use on Surrey or Sussex 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 may lead to the unauthorised disclosure police information if lost or stolen. It is essential you do not upload sensitive or evidential data on unencrypted devices unless explicitly authorised by Security and Information Assurance.

Encrypted USB memory sticks may be obtained from the IT Department, following your manager's approval, which you will be asked to cite. **All data must be deleted from the USB as soon as possible after its policing purpose has expired.**

An encrypted USB memory stick can be used to store information with a security classification of **OFFICIAL**.

If you lose your portable device you must immediately inform the **IT Service Desk immediately** on 01273 635145 or via the Self Service Portal on the intranet, and complete the Security and Breach Reporting form.

Remote Working

Remote Working is defined as any time you are working away from a Surrey or Sussex Police occupied site.

Only use equipment issued to you by the Force to access Police systems and information. Use of privately owned equipment is prohibited. **Remember the following:**

- Ensure that your Force laptop or mobile data device is disconnected from the Remote Access connection when unattended
- Your Secure RSA token/ VPN card must not be kept with your laptop
- Do not write your PIN down (Tokens/cards are assigned to individuals and are not to be shared)
- Under no circumstances should you divulge log in details, passcode details or provide the token/card to any other person
- Always make an assessment of your surroundings, screen filters must be used in public areas, or where you can be overlooked
- Always consider the security classification of the information you are working on and handle in line with Force policies and procedures
- Notify the IT Department immediately in the event of any IT Security incident including compromise, loss or theft of a Force laptop, mobile data device or Secure RSA token/ VPN card
- Keep IT devices physically safe when in transit and securely store all papers and portable IT equipment when work is finished, only take home what is necessary for your task
- Plug your device into the Force network at least once a month to allow system and Anti-Virus updates
- Mobile devices must not be taken abroad without prior authorisation from the Information Security and Special Branch
- Ensure that removable media containing force information is encrypted
- Bring classified information back into the office for secure disposal if there is no approved secure destruction facility available
- Do not work on or store personal data or classified data on personal equipment. This includes PCs, laptops, tablets, CDs, DVDs, memory sticks etc.

When working from home it is your responsibility to make sure information is safe and that your household understands the need for the security measures to be taken.

Your line manager may need to conduct a security assessment of your home working environment if the home-working arrangement is frequent or long term.

You should not send or forward Police business-related e-mail documents or other Police information to personal home e-mail accounts.

You should be aware that there are inherent risks when sending e-mails to your home computer and that 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. 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 and Sussex 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.

Resources

Remote and Home Working Procedure

Market Place

Market Place is used by Surrey and Sussex Police employees to advertise goods for sale. Market Place must only be used to advertise **your privately owned** goods for sale or property to buy/rent/let or to request wanted items.

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

If you are posting Services, Property or Holiday adverts, you will need to have a valid Business Interest registered.

Contact: BusinessInterests.Vetting@sussex.police.uk

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 under the Criminal Justice and Public Order Act, which states 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 Market Place to gain sponsorship for charitable work (for example the London Marathon or fun runs), is permitted.

Links to charity websites are not permitted.

Surrey and Sussex Police do not endorse or accept liability for any items advertised on Market Place.

Adverts must not contravene any part of the Use of Email Procedure

Any failure to observe these requirements will automatically result in the deletion of the Market Place advertisement, 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 and Sussex Police
4. Your current performance
5. Your health, safety and well-being.

The full Business Interest and Additional Work Policy can be found here.

ID-Access and Contractors

Access cards are used to ensure that only authorised people can access Surrey or Sussex Police buildings. In the interests of security, identity cards **MUST** be worn, and clearly visible at all times whilst on Surrey or Sussex 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 and Sussex 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 or Sussex Police staff or other non-employee, be allowed to be passed or loaned to any other person to gain access to 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 Access Card Enquiries (Surrey) or HQ Reception (Sussex) immediately so that the system can be updated to prevent any further access. You can do this by emailing the relevant force's access card department or by filling out a Security and Breach Reporting form.

You must also inform, in writing, your Line Manager or Departmental Head (Surrey) or the Estates and Facilities Helpdesk (Sussex).

In the event you lose your card out of office hours, you will need to inform the Force Control Room who will be able to block your card.

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

Please do not get offended if you are asked to prove who you are. All employees are empowered, and expected, to politely challenge persons on Surrey or Sussex Police premises not displaying appropriate identification.

Visitors and Contractors

Visitors to Headquarters

Visitors to Police stations and other Police sites must comply with local directions or instructions.

You should inform Reception of any visitors to HQ prior to arrival by either email (Sussex) or the Visitors Form (Surrey).

On Arrival

All visitors must report to Reception to be greeted, signed in and relevant documentation checked. They will then be asked to wait until someone can collect them.

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

In Surrey, 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 lanyard** unescorted within secure areas, you are **encouraged to challenge** the visitor to ensure that they comply with this procedure. You can check with reception team or alternatively, you can seek assistance from the nearest department to help verify the visitor.

In Sussex, visitors will be given a visitor pass.

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

On Departure

All visitors to either force must report to Reception to sign out and hand in their pass.

The '**Escorted**' visitors must be escorted back to reception. The Reception officer will then sign out the visitor on the register.

Visitors to Surrey Police Headquarters

Visitors from Other Forces

- Must report to Reception and sign in as a visitor
- 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 **Car park permit** (issued by the reception team)
- This must be clearly seen so they can be contacted quickly if necessary.

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.

Electric Cars

- There are a number of spaces with charging points at Surrey HQ which are dedicated to electric cars.
- These however are restricted to force issued/fleet vehicles only, and cannot be used by employees with their own personal electric car.

Changes in your Circumstances

When you first join Surrey or Sussex 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
- Change of address
- Change of co-residents
- Criminal offences or associations
- Financial circumstances
- Any other risk factor that could potentially impact upon your vetting clearance

You can report relevant changes to Force Vetting. Please be assured that all 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 Manager, 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. This is to reinforce the requirement that the actions of Surrey and Sussex 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 or Sussex Police**.

Drugs and Alcohol

Surrey and Sussex Police seek to provide a safe, healthy and productive working environment for its police officers and staff where alcohol and substance misuse will not be tolerated, however, we will offer support to individuals who voluntarily seek help prior to undergoing any test procedure.

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

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 assistance. 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 personal responsibility to acknowledge your condition and seek assistance.

Where employees recognise that they need help, the primary aim of the service will be to support and assist that person. The overriding aim is to achieve a full recovery, thereby allowing a return to work to undertake the normal range of duties.

However, any such self-declaration must be made before a notification of any requirement to take a test and individuals who self-declare will still be subject of investigation if their behaviour breaches the standards expected of them, for example, attending work under the influence of drink or drugs.

Police officers and staff in safety critical or vulnerable roles may be subject to regular substance testing. The force also has the power to test any officer or staff member if there is cause to suspect that they are misusing controlled substances.

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

Resources

Surrey: Alcohol, Drug and Substance Misuse by Officers and Staff Procedure

Sussex: Substance Misuse and Testing Policy (Including Alcohol and Drugs)

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, you and the organisation should be protected 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.

For example, a relationship between a manager and a subordinate could lead to favouritism in a promotion process, over equally or more capable members of the team.

Examples of activities where conflicts could arise are:

- Performance assessments
- Promotion/selection procedures
- Pay decisions
- See the Disciplinary Policies
- See the joint Workplace Resolution Procedure
- 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 Force 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 or Sussex 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 Force 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 Gifts and Hospitality application form to BusinessInterests.Vetting@sussex.police.uk who will provide you with guidance and advice.

Resources

Anti-Fraud, Corruption and Bribery Procedure

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 or Sussex 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 or Sussex Police are significant.

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

Removing Security Classified Documents from Police Premises

On occasions you may be required to remove physical 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.

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 or Sussex 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. 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 security classified document. If a computer is to be used for such material, it must be authorised, issued and approved by IT.

It is critical all Force employees, volunteers, contractors understand this.

Resources

Government Security Classification Guidance

Travelling on the Surrey or Sussex Police Minibus

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

Keep in mind that occasionally members of the public travel on the bus and should not be exposed to sensitive or restricted Police information.

'Social Engineering' 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 system for Surrey Police Officers and Staff which enables messages to be exchanged directly with the Anti-Corruption Unit anonymously. The purpose of this system is to provide a way for all employees to report corruption, misconduct and other inappropriate behaviour 100% anonymously. We all have a responsibility to report any wrongdoing we discover and not fulfilling that responsibility effectively condones that behaviour.

Reporting concerns to the Anti-Corruption Unit is best done directly in person or over the phone, but this system is available to all officers and staff to ensure that these matters can be reported even if the person is fearful of coming forward.

To access the system, simply type the word “anonymous” into the address bar in the internet browser on your work computer/laptop and follow the instructions. You can also click the link at the bottom of the home page on the force intranet under the heading Tell PSD anonymously (this also works on an MDT).

All submissions come directly to the Anti-Corruption Unit who will read, assess and respond. In order to view these responses, you will need to make a note of your unique ID and know the password you set with the first message in this thread. As the system is 100% anonymous, passwords and lost usernames cannot be reset.

In order to offer people the highest levels of protection when they come forward, the Anti-Corruption Unit will always ask if users of the anonymous system are willing to come forward in confidence to us. People who approach the Anti-Corruption Unit directly (including those who later come forward having first used this system) are afforded protection in line with the force whistleblowing policy to help ensure doing the right thing does not adversely affect them now or in the future.

By providing information about corruption and wrongdoing, officers and staff are able to help protect members of the public, the integrity of the force and policing in the UK as a whole.

Break the Silence

Breaking the Silence offers all Sussex Police Officers and Staff the opportunity to securely report any concern in the strictest of confidence.

The system is maintained by the PSD Anti-Corruption Unit and is used by colleagues on a daily basis. The team receives in excess of 300 communications each year and is recognised both regionally and nationally as 'best practice' in making protected disclosures (Whistle Blowing).

If you have any integrity, corruption or misconduct-based concerns which are likely to have reputational issues or impact on public safety, then this service offers you a viable alternative to reporting your concerns via local supervisor.

The integrity of 'Break the Silence' has never previously been compromised, hence you are urged to communicate ANY concerns you have which will be considered by PSD.

Any protected disclosure will be recorded and assessed by suitably trained staff with a response posted within 24 hours (excluding weekends). You may be asked for more details, but this is normal practice and allows officers the opportunity to make a more informed assessment of your information. PSD will ensure that your concerns are fully considered and communicated to an appropriate authority best placed to manage them in confidence.

Whistle Blowing

All Surrey and Sussex Police employees have responsibility to report any dishonest, corrupt or unethical behaviour in the workplace.

Any individual who carries out a dishonest, corrupt or unethical action compromises the high standards of Surrey and Sussex Police, and potentially damages public confidence. Any individual, who knows or suspects a colleague to be acting this way and does nothing effectively condones the activity. This in turn opens up to criticism the reputation of every other colleague as well as that of themselves and could lead to disciplinary action being taken.

Reports can be made to:

- PSD Anti-Corruption Unit
- Staff Associations
- Crimestoppers 0800 555 111
- IOPC Report Line 0845 8770 061
- Anonymous (Surrey)
- Break the Silence (Sussex)

A person who makes a protected disclosure is a whistle blower and has the right not to be dismissed or subjected to victimisation because they have made the disclosure. However, just because a person blows the whistle does not make them immune from any disciplinary action.

Anti-Corruption Units recognise the fact that there may be circumstances where the person is reporting an issue of concern may wish their involvement with PSD to remain on a confidential basis e.g. where there is a risk to personal safety, or where disclosure would have a serious detrimental effect on the quality of life in the domestic or workplace environment.

Police officers and police staff should contact PSD so that matters of confidentiality can be discussed. Decisions regarding confidentiality will be managed sensitively by PSD and the person making the report will be kept fully informed of any decisions made in relation to the disclosure.

There may be occasions where an officer or member of staff does not feel that they can openly report their concerns and therefore, an anonymous method of reporting concerns to either PSD Unit is provided.

Anti-Fraud, Corruption and Bribery Policy

Useful Contact Details

IT Service Desk

IT Service Desk

Self Service Portal

Force Vetting

Force Vetting

Information Security

Information Security

Data Protection

Data Protection (Surrey)

DPO (Sussex)

Occupational Health

Occupational Health