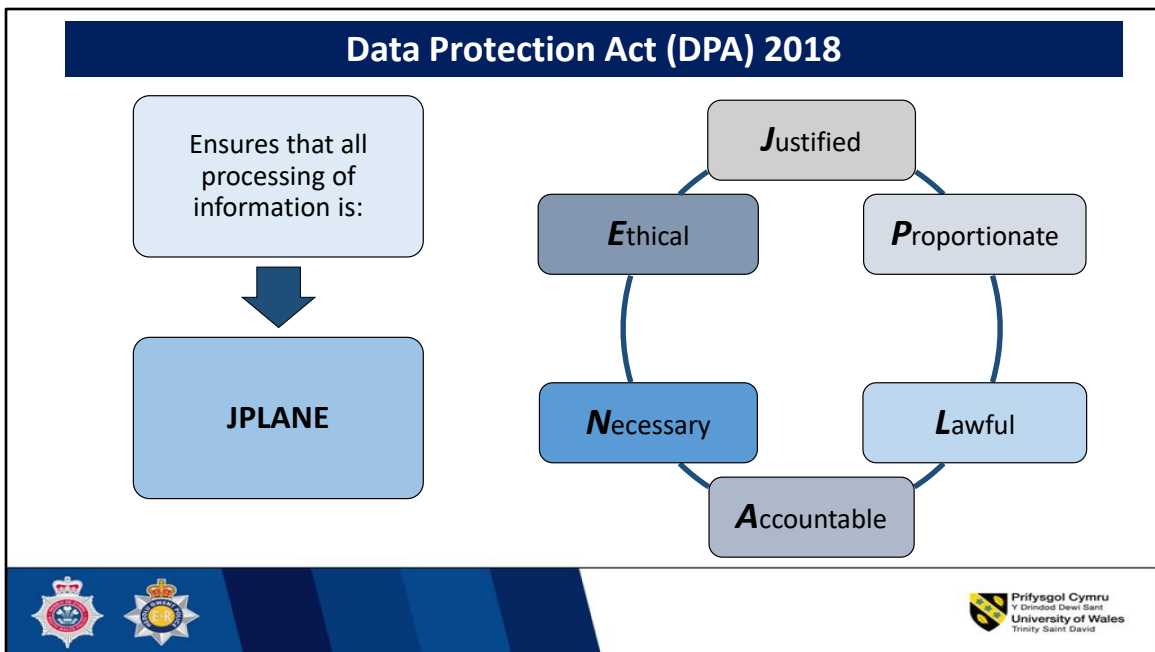




By the end of the lesson learners will be able to:

1. **State** why data protection is important
2. **Explain** what personal data includes
3. **Explain** the Data Protection Principles
4. **Explain** the Freedom of Information Act
5. **State** what security measures can help secure our information



You may have heard of JPLANE in policing – this applies to processing personal data too.

As personal data is increasingly stored, processed and exchanged on the internet and as such often exists in an international environment, this Act was introduced to interlock the UK's data protection laws with international data protection arrangements. It replaces the Data Protection Act 1998 Act and provides a comprehensive legal framework for data protection in the UK, in accordance with the General Data Protection Regulation ((EU) 2016/679) ("GDPR").

The Data Protection Act 2018 is structured into seven parts:

Part 1 contains preliminary matters which include an overview of the Act and defines terms used throughout.

Part 2 must be read alongside the [GDPR](#) and sets out certain derogations from the GDPR. It also contains provisions extending the GDPR standards to areas outside EU competence (the "applied GDPR" scheme), with the exception of law enforcement and processing by the intelligence services.

Part 3 makes provision about the processing of personal data by competent authorities for law enforcement purposes and implements the [Law Enforcement Directive](#).

Part 4 makes provision about the processing of personal data by the intelligence services.

Part 5 makes provisions about the Information Commissioner.

Part 6 makes provision about the enforcement of offences

Part 7 makes supplementary provision, including provision about the application of this Act to the Crown and to Parliament

Why is the Data Protection Act important to you?

The criminal offences created under the Act make the Chief Constable (the data controller), or **you** (as their servant) individually liable



You are liable for any deliberate infringements



You have a responsibility to make sure that you comply with the Data Protection Principles



QTS - When do you hear the term 'data protection'?

As well as preventing someone obtaining personal data about a third party the data protection goes beyond that and covers aspects such as data security and data accuracy and affords certain rights to individuals, which we will look at in more detail.

So in this slide you can see officers raiding a house. But what if it's the wrong house? What if the intelligence has been put on the wrong address, and actually they should be conducting the raid next door? What would the consequences be? the occupier would be entitled to compensation

The person who should have been subject of the raid could become suspicious that the police know about their illegal activities and could remove all the evidence which would ruin the whole operation which would result in a waste of time and resources.

Again, the second slide shows someone being arrested. A wrongful arrest due to inaccurate data is likely to result in a compensation pay out as if an individual suffers any damage or distress as a result of a breach of the data protection act they are entitled to compensation.

SWP pay out in excess of £20,000 a year compensation for wrongful arrests

Why is the Data Protection Act important to the Police?

The Police holds a great amount of sensitive information about individuals for policing & employment purposes.



It needs '**protecting**' to ensure that:

- It is not misused.
- It is accurate, adequate, relevant & not excessive.
- It is not inappropriately disclosed
- It is kept secure

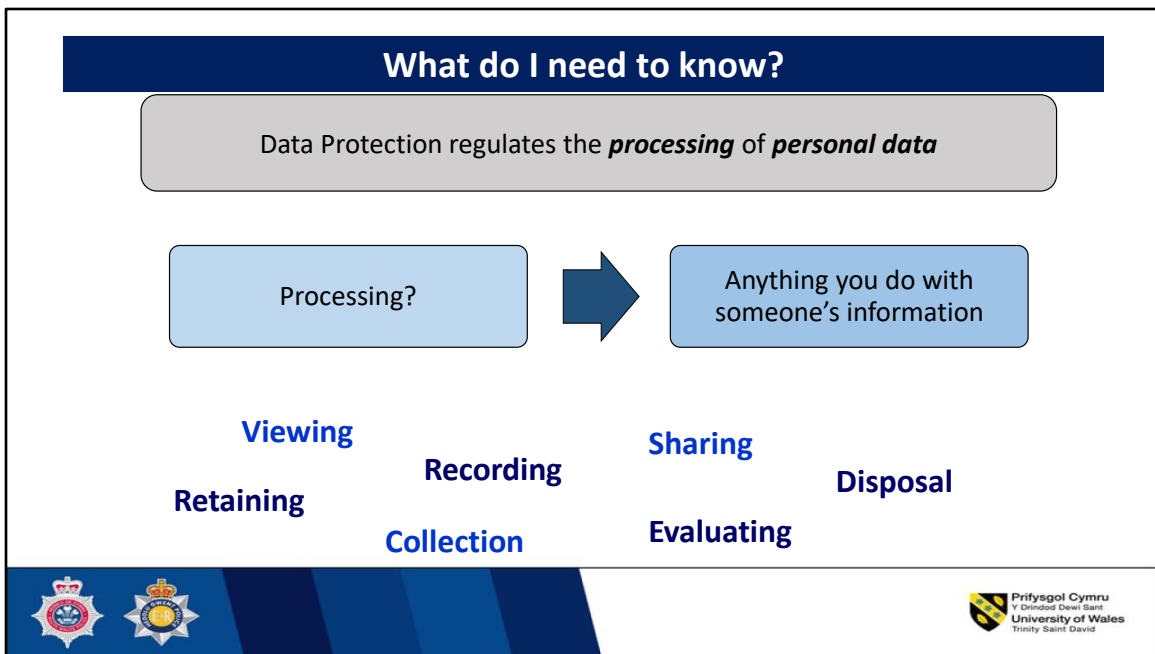


QTS – Why is Data Protection important to you and the Police?

DP regulates how information is used. All **your** personal information is being used and you want it to be protected.

For example, SWP hold information about you in their personnel files. Some of this information can be quite sensitive (ie how much you earn, whether you have any disabilities, your sickness record, your sexual orientation. You would not want that information shared with people that didn't need to know!!) Illegal activities such as fraud can take place as a result of the gain of the personal data of others. SWP have a legal duty to protect this information (therefore, SWP would only disclose information about employment or pay details for a mortgage application for example, with your consent).

It is obvious that SWP hold personal data which is sensitive and could have serious consequences if lost or inappropriately disclosed.



QTS - Can anyone give me any examples of processing?

On 25 May 2018, the General Data Protection Regulation, otherwise known as GDPR, replaced the current Data Protection Act 1998. The GDPR is an EU regulation, which seeks to harmonise the rights, protections and remedies of all EU citizens in relation to the processing of their personal data.

The **GDPR** specifically excludes processing personal data for the purpose of law enforcement, but a new piece of legislation came into effect on 6th May 2018 called the Law Enforcement Directive (LED).

These, along with the processing of data for national security matters, are covered across the UK by a new Data Protection Bill, and has now formed the new **Data Protection Act 2018**.

Described under these changes as the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties and includes safeguarding against and the prevention of threats to public security; the 'law enforcement' element of our work will fall under the new Act. The remainder of our business will fall under GDPR and whilst the provisions of both are similar there are

some important differences.

The police service has to comply with the GDPR, the Law Enforcement **and**, the new Data Protection Act 2018. This is because the police service processes personal data for a number of business purposes other than law enforcement, such as HR and Finance. It is going to feel a bit strange at first with some areas of business working to different legislation for data protection purposes.

Relationships and arrangements with partners and other agencies, particularly in relation to information sharing, will continue into the future albeit there will no doubt be a need to make some practical adjustments in order to achieve and demonstrate compliance. This area will be informed by NPCC and other national guidance and by developing a shared understanding and approach with our partners.

The GDPR introduces an accountability principle which, put simply, means that it is not enough to be compliant; organisations will need to be able to actively demonstrate their compliance through policy, procedures and practice; providing further opportunity to enhance trust and confidence within our communities.

The new Data Protection Act largely mirrors GDPR; the big difference is that it will only relate to the processing of personal data for the purposes of law enforcement and national security.

Data Protection



The UK's independent authority set up to ***uphold information rights in the public interest***, promoting openness by public bodies and data privacy for individuals.

Case Study

CONVICTED: Unlawfully obtaining

Despite the fact he made no known use of the information seen, an employee was convicted of unlawful obtaining of personal data when he accessed records on his employer's computer system for his own purposes and not in the course of his employment.



The FOI and DP Acts are regulated by the Information Commissioners Office. They deal with any queries, appeals against disclosure decisions, complaints and breaches of either Act. This applies to any organisation or company that processes personal data, from the NHS and Police Service, to companies like Halfords or Currys who may hold information such as your address and details of hire purchases. The ICO have the power to step in and investigate any issues. They can prosecute, issue fines and enforcement notices.

Examples of accidental breaches:

- Posting a victim contact letter or a payslip to the wrong address,
- Emailing CRB database or sickness info to the wrong address (give Gwent CRB example)
- Dropping papers on the floor
- Leaving files or notebooks on a train
- Disclosing pre-cons to the Courts from the incorrect record

Then you have the breaches where systems are accessed for personal reasons. As well as being unethical, this is a breach of the Data Protection Act and cases will be investigated and dealt with by Professional Standards.

The more serious breaches are deliberate such as accessing systems with the aim to

sell the information or use it against someone else. There have been a few cases of these, some in South Wales in recent years.

Now we will take a look at some recent fines issued by the ICO

Fines issued under the Data Protection Act

£160,000

SWP fined for being unable to locate a DVD of an interview with a victim of sexual abuse. The DVD has never been found

£180,000

The Serious Fraud Office fines after a witness was mistakenly sent evidence relating to 64 other people involved in the case

£100,000

Kent Police fined for leaving sensitive & confidential information including interview tapes in a basement of a former police station

£150,000

Glasgow City Council fined after 2 unencrypted laptops containing personal data were stolen during an office move after an employee forgot to lock a cabinet



Here are some examples of fines issued by the ICO under the Data Protection Act. Fines can currently go up to a maximum of £500,000)

A lot of these fines are solely due to one individual being careless. I personally would not want to be the person who is responsible for a fine during times where jobs are being cut in order to make savings. Please look after other peoples information! In these cases the force has been responsible for paying the fine, but if you sell or deliberately obtain personal data unlawfully - you can be personally liable for the fine. The most common type of breaches we deal in the Data Protection arena are the loss of information, inappropriate disclosure and sending information to the wrong recipient.

Although the DVD in the case of SWP has not been found and it could well be still within the possession of SWP, the victim has to live with the fact that an unencrypted video recording lasting over 2 hours showing her recounting harrowing details of childhood sexual abuse could turn up anywhere. The fine was so high because the department who lost the DVD did not internally report the matter as a data breach, and the Data Protection Office only found out about it when the victim wrote to PSD to complain two years later.

The ICO Decision notice specifically made reference to the fact that the investigating officers line manager was not aware of the procedure for reporting data losses. I cannot stress enough that all data losses or breaches must be reported to the Data Protection Office via the online tool on the front page of BOB, who will decide whether further reporting or further action is appropriate. There is now a specific procedure in relation to the storage and destruction of Dvds which can be found on the SWP intranet. Kent Police – the contents of the victim's phone including photos were passed to the suspect by mistake, who was a serving officer undergoing a disciplinary at the time. Although this was due to human error, as you can imagine this caused the victim serious distress.

Dyfed Powys were fined £150,000 in 2016 when a total of five emails were sent to the member of the public all containing personal data after their details were added to their 'global address book'

So all of these are 'accidental breaches'.

Police Checks on Partners Broke Data Laws (BBC, February 2013)

Police officers & staff in Wales have broken the DPA 62 times in the past two years.

4 people were sacked & 14 resigned as a result of their actions.

The breaches included checks on partners, relatives & associates, altering their own records, & passing data to third parties.

The Information Commissioners Office said:

"We expect police forces to make substantial proactive efforts to check that any access to their records is for legitimate police purposes & to take action where they discover wrongdoing."

Public officials who abuse their positions can face serious consequences including criminal prosecution under the Data Protection Act."



Examples of breaches

Ⓢ1MONⓈ

Vehicles:

ⓈA1COPⓈ

People:









QTS – Can anyone give me any examples of where officers may breach the DPA & acquire information they shouldn't?

Some more examples of breach of the act are, using PNC or Niche to check the owners of personalised number plates in order to approach them for a sale, to find out what offences the driver may have committed, or if they have seen their son or daughter in a vehicle and they check who the owner is to find out who they are associating with. VRMS can identify a person therefore they fall within the definition of personal data!

Again, there is a huge interest in celebrities and their private lives, so obviously you must not look at the record of Ian Watkins or any incidents involving the Welsh Rugby Team or footballers for example. Even if you are just viewing this information and do not do anything else with it you are breaking the law and putting your job at risk.

You may think accessing information about yourself as a person reporting a crime for example doesn't count as a DP breach as you have given yourself consent to do so – however as well as being unethical you are still accessing information which is not for a policing purpose and this will be dealt with very seriously.

Data Protection

BBC NEWS

A FORMER head of South Wales CID was jailed after admitting paying contacts to supply his private investigation agency with information from police & government databases.



Here is an example of one of the more serious breaches. You cannot actually receive a prison sentence for breaching the Data Protection Act. The worst penalty is a fine, but in cases such as these other offences are made out, such as fraud and misconduct in a public office.

Philip Jones, 63, retired as a Detective Chief Superintendent in 1997 after 30 years service.

He then launched a private investigations agency and persuaded former colleague David Lloyd, 55, to pass him information from police computer systems.

Jones also used freelance investigator Christopher Barnett, 37, to illegally pose as a customer to gain information from government and private institutions. The former top detective, who headed South Wales CID until his retirement in 1997, admitted conspiracy to commit wilful misconduct in a public office and conspiracy to commit fraud by false representation at Bristol Crown Court in December 2008

Jailing Jones for 18 months at the same court, Judge Simon Darwall Smith slammed his behaviour as “corrupt” and criticised his “lack of moral fibre”.

What is 'Personal Data'?

Data that:		
Relates to a living individual who can be identified from that information	Or indirectly from that information & other information likely to come into your possession	And includes expression of opinion & intentions



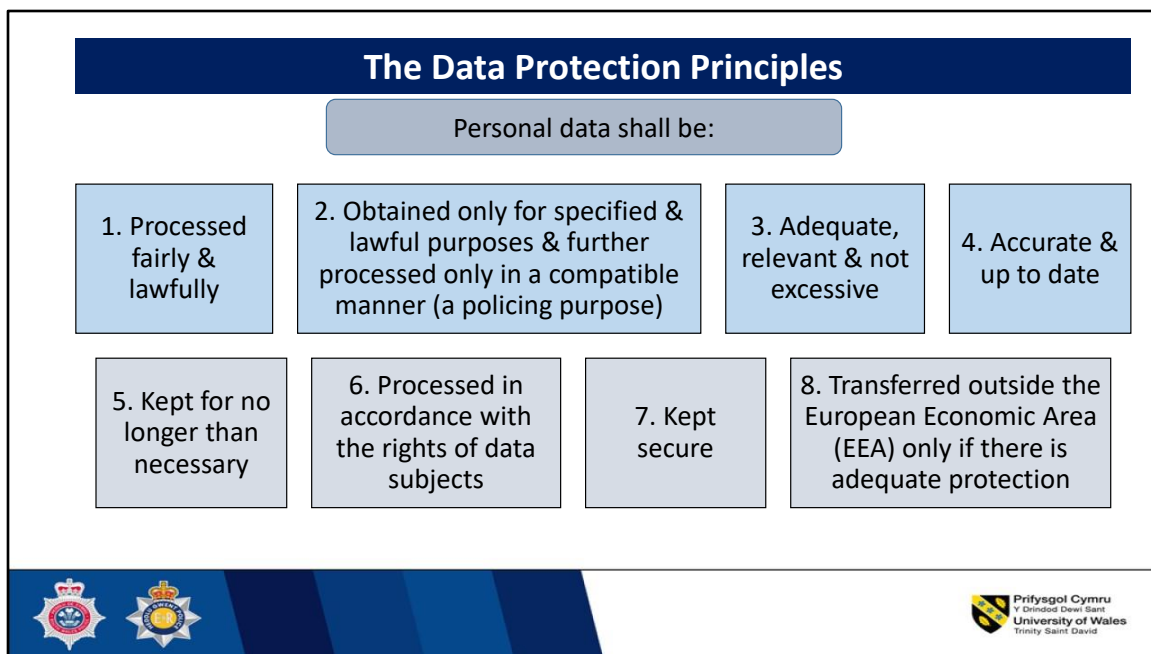
QTS – what is personal data?

The Act states personal data must be protected. Personal data is any information that relates to an individual who can be identified from that information – so, someone's name, address, photograph, convictions, intelligence, etc are personal data. It's easier to remember that it protects information that "belongs" to that person.

Also, the Act goes on to cover data which isn't obviously personal data. So information such as a bank account number or a fingerprint obtained from a scene of a crime, by itself would be meaningless. However, we found out who that number belongs to (via bank) or input the fingerprint onto the Fingerprint database then it is likely that we would identify an individual, therefore, all this type of information is personal data too. This applies to occurrence numbers as an individual could be identified from that information.

Finally, the Act states that expressions of opinion are personal data. Therefore, if you wrote in an email or in your pocket notebook "Mrs Jones is a nutter or an psycho" – this would all constitute personal data protected by the Act and therefore relevant for disclosure to Mrs Jones if she applied for it. If we are going to record this type of information about identifiable individuals, we must comply with the principles of DP.

This does not mean that you cannot record opinions, just keep them professional, unambiguous and make sure that it is clear that it is just an opinion and not fact.



These are the 8 principles of the Data Protection Act.

The force (or any organisation that uses data) must comply with every single one of the principles, if we fail to comply then the processing will be unlawful and if an individual suffers any damage or distress as a result of that processing they would be entitled to compensation!!

Principle 1 - the most important. As in order to comply with the other 7 principles you must have obtained and processed the information lawfully. If you have not done then there is no point even thinking about the other principles as you are already breaking the law. The second principle is the one which is most often breached, not using or processing the data for the reason for which it was obtained.

Principle 2 - Can anyone give us some examples of personal data you process in your roles?? And can you identify the wider 'policing purpose' for this processing? Ultimately why do you carry out this work? (see next slide)

Principle 3 – Information must be necessary for police work. Not too much a problem to comply with this principle as a lot of information may be relevant for police work. ie. we obtain information of shoe size, eye colour, left/right handedness, etc.

All reasonable for police work but excessive to open bank account, etc as there is no need for these details to be given. Insurance company ask smoker/non smoker, married/single, what credit cards you have, etc WHY?? It may be worth asking.

Would you really need to record that someone is ugly or smelly? – maybe you would need to record smelly if there was a concern for their health or wellbeing

A ruling in the 90's ruled that HIV markers could only be entered if there was a valid policing purpose, so a marker can only be entered if that person is a real threat to others, for example if they threaten to stab officers with dirty needles. The Data Protection Office carries out an audit on HIV Markers, and if they are not for a valid purpose, they are deleted. Officers should act with caution whenever they come into contact with bodily fluid, it should not make a difference whether that person has a HIV marker or not.

Any disclosure must be relevant and not excessive – otherwise there will be a breach of this principle

Principle 4 – Must keep information accurate – straightforward! – data quality.

Example of problem is warrants not cancelled on PNC, intelligence or arrests put on the wrong person record, and as you can see in the poster – wrong dates of birth Up to date – if we record someone as heavy build and they lose a lot of weight, they could ask us to alter the description of them. In order to comply with this principle, we would need to update the record.

Principle 5 - Kept for no longer than necessary.

We have retention guidelines on how long data should be kept which can be found on FIS.

We also have a MOPI (Management of Police Information) team of retention and disposal officers going through all old records to determine whether they still hold value for a policing purpose, and if not then it is deleted

Principle 6 - You should be aware of what a subject access request or 'data protection check' is. A subject access request entitles an individual to know what personal information is being processed in relation to them.

Individuals can apply for any information held about them. The most common ones that we receive are PNC and niche occurrences but we also receive requests for CCTV, occupational health records, interview recordings, photos taken in custody and I have even seen a request for a DNA profile.

This is not the process which should be followed if a person wishes to apply for a job and needs to provide evidence of any criminal record, or lack of. If that's the case they need to apply online to disclosure Scotland.

Anything you record about someone could be disclosed to them if they made a subject access request – even your opinion!

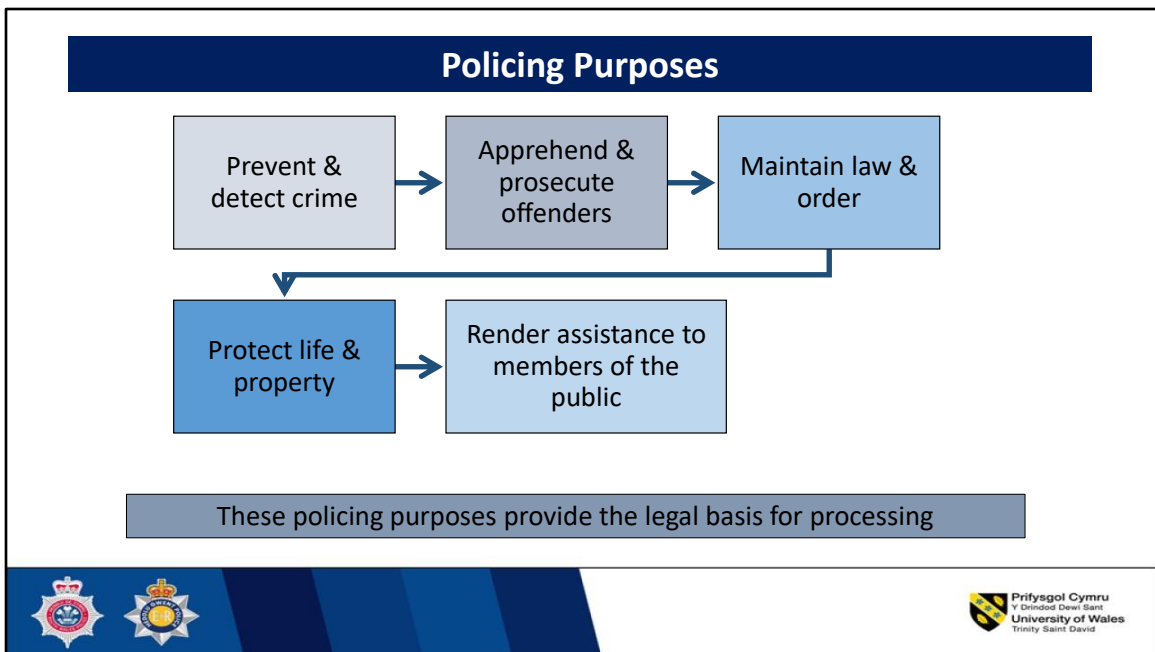
Any questions?

Principle 7 - Kept secure

We have a Force Information Security Officer assigned to ensure compliance with this

principle and we have a section on this later where we will talk more about this.
(We shall look at this in more depth further on in the lesson)

Principle 8 - transferred outside the EEA only if there is adequate protection.
Some countries outside the EEA don't have the same or any data protections laws.
So you are responsible for ensuring that the data will remain protected if you transferred it elsewhere.



QTS - What is a “Policing Purpose?”

Information can only be used for this one purpose, the policing purpose which is mainly seen as the prevention detection of crime and the apprehension and prosecution of offenders but also to maintain law and order, protect life and property and render assistance to member of the public. So there you have the legal basis for processing.

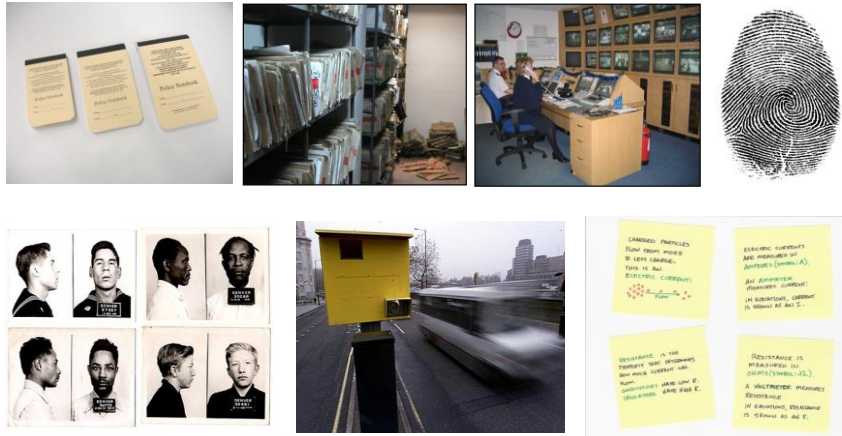
The Data Protection Office frequently carry out monitoring checks on what transactions are undertaken and officers are randomly sent memos asking for evidence that checks are for policing purposes. If it is found that checks are unlawful then there is a possibility that officer will be dealt with accordingly.

Only use information for legitimate policing duties, if in doubt ask!

The same goes for other organisations such as social services, NHS, insurance companies, that are asked by a member of SWP to supply information, they must be sure that the information is going to be used for a policing purpose. If you require information from any third party then you must complete and submit a Personal Data Request form which has been signed by a supervisor.

If you are asked to disclosure personal data consider – would the data subject reasonably expect me to disclose this information?

It's not just information on computers!



QTS – What other types of information can be held, apart from information on computers?

As mentioned earlier the Act covers all types of information, PNBs, paper files, CCTV, prints, DNA, Photos, recordings from speed cameras and even information recorded on post it notes and we must apply the data protection principles to all this information. So please, for your own sake ensure that you protect this data and that you are professional and accurate when recording anything.

Any question so far?

Remember

Ensure you are accessing data on a **need to know** not **nice to know**
basis

NEED TO KNOW



Finally READ SLIDE That's the end of the DP section. Any questions before I move onto Freedom of Information?

Freedom of Information Act 2000



QTS – What is the Freedom of Information Act?

You may have seen news articles about Prince Charles letters to government being published? That was all due to an FOI request.

Q. What is the Freedom of Information Act?

It gives the public a general right of access to information held by public authorities.
An act to make provision for disclosure of information held by public authorities or by persons providing services for them.
Deals with access to official information that is recorded by a public authority.
Aimed at making public authorities open, transparent and accountable

What is the Freedom of Information Act?

Aimed at making public authorities open, transparent & accountable

Gives members of the public access to a much wider range of information through the '**General Right of Access**'

Right to know if information exists

Right to be provided with that information within 20 working days

All organisations **must** have a 'publication scheme'



It gives the public a general right of access to information held by public authorities.

The Freedom of Information Act came into force at the beginning of 2005 – since then all requests received by a public authority have to be answered in accordance with the act.

Freedom of Information Act is an act to make provision for disclosure of information held by public authorities or by persons providing services for them.

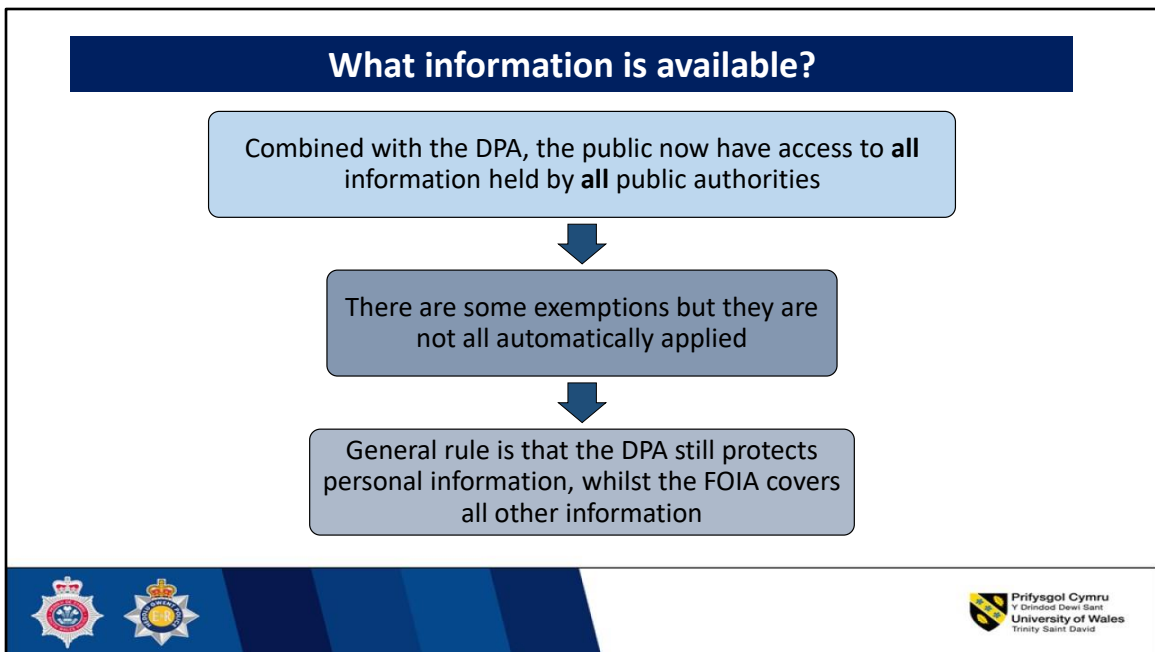
The Freedom of Information Act deals with access to official information that is recorded by a public authority.

Freedom of Information requests can be for written documents, either manual or electronic, pocket books and notebooks, videos, tapes or even information stored by private contractors on behalf of the force.

The public authority has 20 working days to respond to a request – this includes retrieving the information from the business expert (department) reviewing and analysing the info received and applying any exemptions that are applicable.

South Wales Police along with all other public authorities must have a publication scheme. The scheme sets out numerous requirements for proactively publishing information on our website in order to be open and transparent, such as gifts and hospitalities, minutes of meetings, chief officer expenses, contracts, spend over £500 and many others.

Applicants are sometimes directed to the website before making an FOI request.



Everyone has had access to information about themselves through the DPA for many years.

FOI does not cover personal information - this is exempt under the act. So you cannot receive information about someone else through this legislation

In some cases information can be withheld; the Freedom of Information Act sets out certain exemptions that authorities can use to decline a request for information; these exemptions do not apply automatically, we must provide evidence which shows that the release of the information would not be in the public interest. For example if the disclosure would negatively effect law enforcement, or a ongoing police investigation

General rule: FOI covers all other info

- audio & video tapes
- photos
- emails
- reports (including drafts)
- minutes (including drafts)
- post it notes or copies of own notes

What does a F.O.I. request look like?

- No set rules
- Must be in writing: e-mail, fax, scribbled notes
- Must be legible
- Must include a name and address for correspondence

However

- They don't have to mention the Act
- They don't have to be in English



Any person can make a request under the Act - there are no restrictions on your age, nationality, or where you live.

All you have to do is write to (or email) the public authority that you think holds the information you want.

When an application is received it is important that certain criteria is met such as the request must be in writing; by email, letter, or fax. It must be clear, concise and must include the name and address of the person making the request.

The act says a request can be scribbled on a piece of paper and as long as we have a name and contact address (post/email) then it is valid.

This differs hugely to DPA as any of those requests must be applied for via a subject access form and a fee and identification must be provided.

There is no charge for information under FOI however we do have a cost limit for responding FOI requests is £450 or 18 hours worth of work. Where it is estimated that the request for information is likely to exceed the statutory cost limit, the request will be refused by the force on the grounds of cost.

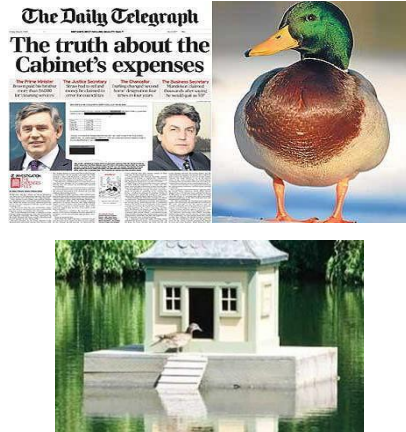
The Freedom of Information Act is purpose blind and applicant blind, this means there does not have to be a specific reason behind the request and it does not matter who makes the request,

- The requestor doesn't have to explain why they want the information
- We can clarify what they want
- Act is fully retrospective
- We must provide the information within 20 working days
- Requests can come from anywhere in the world
- We can't charge people for the information

Examples of requests under the F.O.I. Act

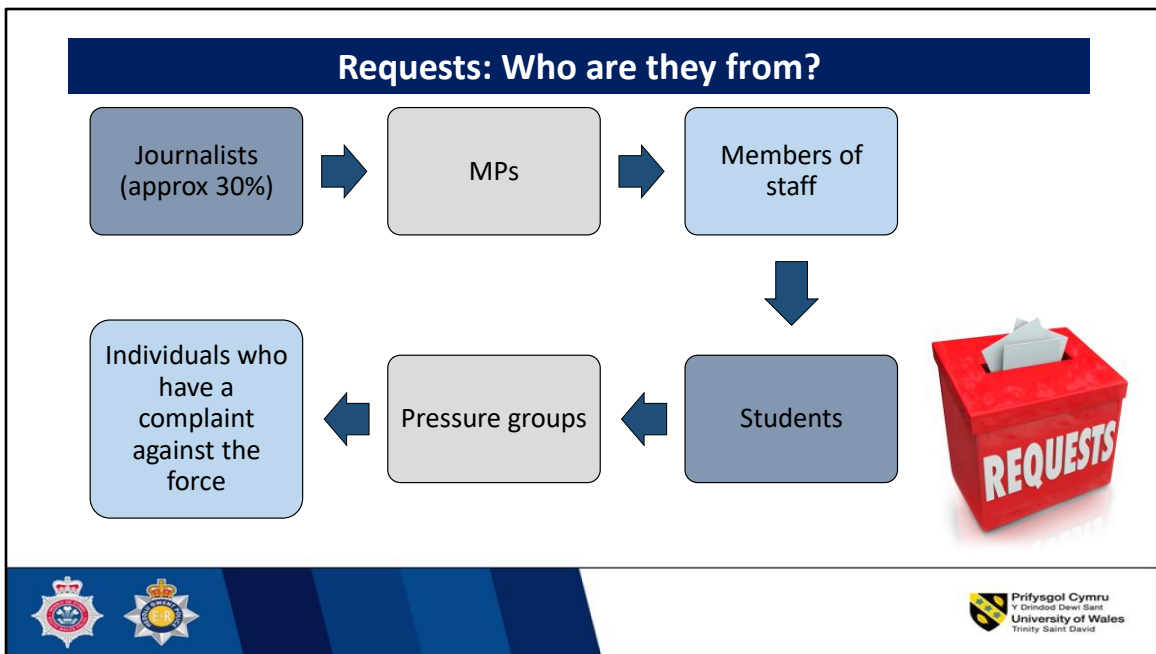
MP's expenses scandal

A claim by Sir Peter Viggers MP for a duck house costing £1,645 came to symbolise the expenses scandal.



You may remember the MP's expenses scandal where details of MPs expense claims were released. The FOI Act is there to make all public figures and authorities transparent and accountable.

More recently – Princes Charles had his letters to Tony Blair disclosed under FOI. In both cases the appropriate bodies tried to block disclosure but the Tribunal ruled that there was no reason why the information should not be disclosed. The government spent around £400,000 trying to fight the case.



Requestors have to give their name and an address for correspondence (e-mail will do), so we won't necessarily know which category they fall under. However, most do specify within the request.

All requests are treated confidentiality, to ensure that info provided is applicant blind – so that basically means that the response will be the same regardless of whether the request comes from an MP or a member of the public.

Freedom of Information Act

GUILTY

It is a ***criminal offence*** for any person to change, erase, destroy or deliberately withhold information to prevent its disclosure under the Act



Say for example, you receive an FOI request for a report you have written on a local policing issue, and there is something in it that you don't really want published as it won't look very good on the either yourself or the force and you then delete a section or shred the report you will be committing a criminal offence.

If anyone is found to have do this, they will be personally prosecuted.

What the exemptions don't cover

Embarrassment

Not being able to find
information we know
should be there

Not having time to look



EMBARRASSMENT

We can't withhold things because they don't look good, or it shows we've done something wrong or because we don't want it to end up in the papers, even if the information is inaccurate. For example we received a request for the number of emergency calls answered within the appropriate time, and due to a technical fault on the recording system some months showed that no calls were answered within the time. This was not accurate, but the legislation covers recorded information, therefore we had to provide the figures and include a caveat to explain the reason for the 0 figures.

NOT BEING ABLE TO FIND

We have no excuse for bad filing or records management: work ongoing!

TIME

We are all busy and all have a "day job": but this is no reason to refuse to provide the information as it is a legal requirement.



Principle 7

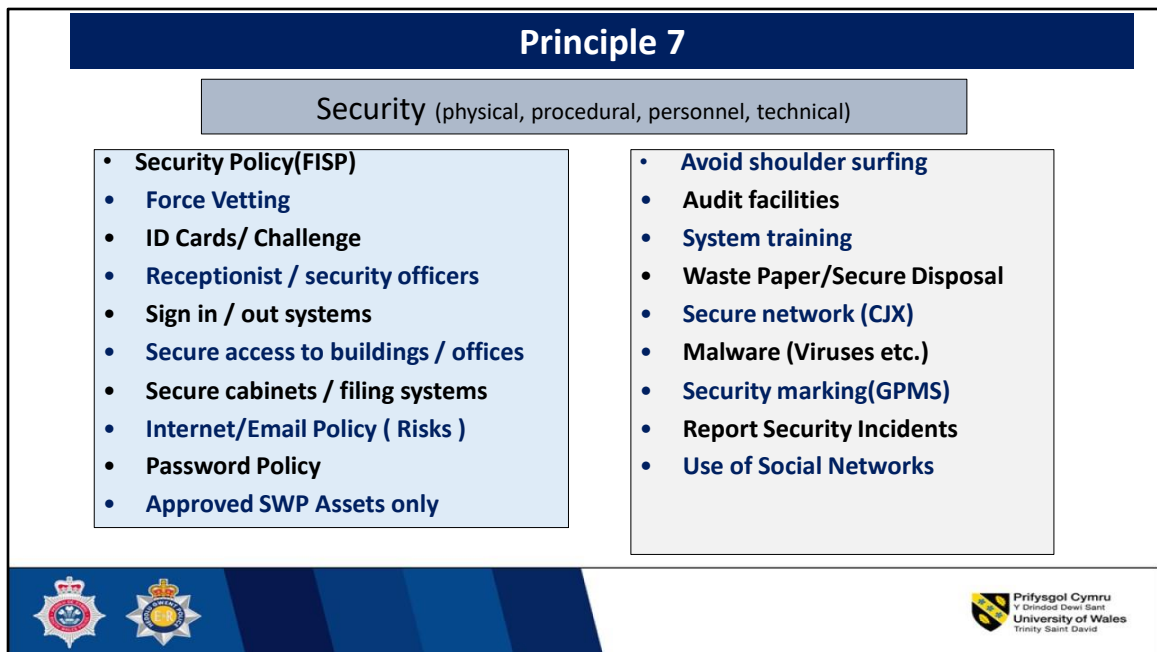
Security (technical & organisational)



What security measures can you think of?



QTS – what security measures can you think of to help secure our information?



Principle 7 – Must have security.

Here are some security measures used. **READ THROUGH and discuss**

Paper containing sensitive or personal information must not be put in normal bins. It must be shredded using a departmental shredder or by placing in one of the approved ‘shred –it’ bags or boxes. Problem with bins being stolen from police stations and paperwork being dropped by the recycling company

Challenge anyone without ID or snooping!! Don’t have monitor facing out window –

It is good practice to ensure your desk is clear of documents at the end of each day and that they are locked away appropriately where possible. Clear desk policy!

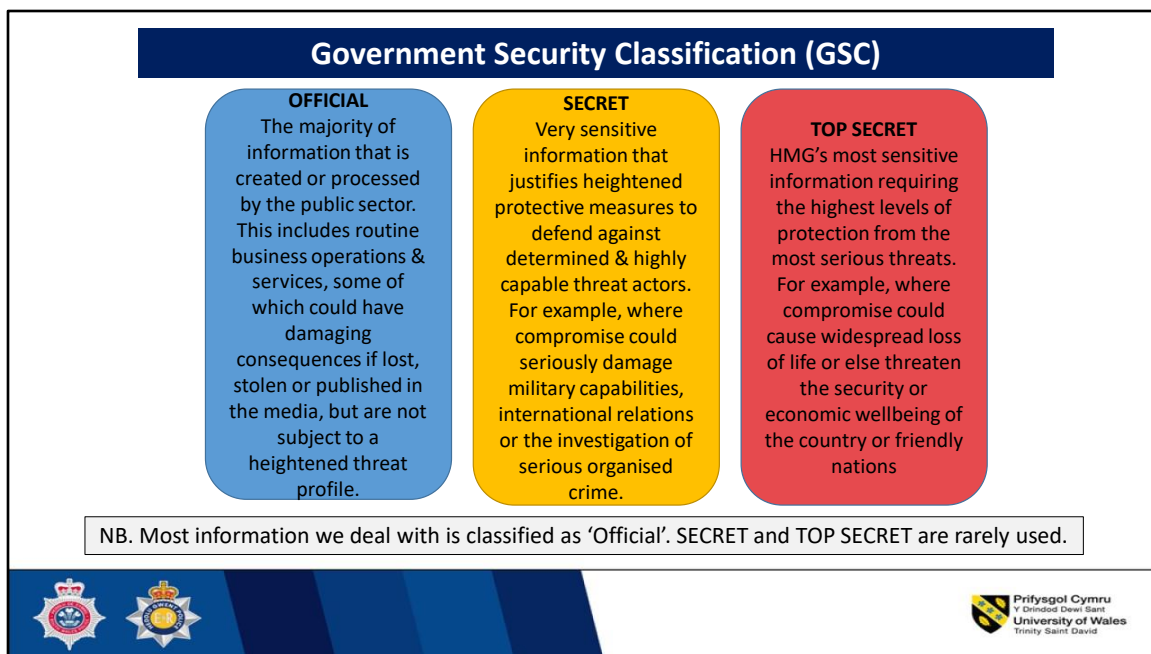
Sharing your password for access to SWP computer systems is strictly forbidden. Problem with laptops and pocket notebooks stolen from cars or left lying about. Do not take work -documents or Dvds out of the office unless absolutely necessary. Risk of breach increases significantly.

Sign work in and out so that it can be tracked down at any time. Bad security!! What would happen to the data if your car was stolen or you were involved in an

accident? What if you were robbed or burgled? Very important – reporting security incidents and data breaches!

ICO fine – again – you must report any security incidents including data breaches and data losses! Even if you lose handwritten notes, if these contain personal or sensitive information you must report it.

Carry notes and files around in a zipped up folder or a locked briefcase. We recently had to report a breach where the wind blew papers out of the hands of an officer and through a street into peoples garden. Not all the papers were recovered and they related to sexual abuse of children. Only take information off site if it is necessary!



Everyone who works with information has a responsibility to safeguard it and to share it with trusted partners outside of the police family if appropriate. The Government Security Classification (GSC) will help you do this.

The GSC was adopted by the Police Service in April 2016.

One of the key messages of GSC is that all information has a value and requires an appropriate degree of protection. These three levels of classification will help you determine the level of protection required.

It is very important that you complete the mandatory NCALT course as soon as you can.

Top 10 Data Protection Tips

1. DON'T access information unless it is for a policing purpose
2. DO record personal data accurately & ensure professional wording
3. BE careful when sending emails
4. USE secure email whenever possible
5. DON'T share passwords
6. DON'T leave your screen unlocked
7. DO follow relevant information sharing agreements
8. DO comply with the retention rules for personal data
9. DO try to keep a clear desk
10. DO treat personal data carefully and look after it – REPORT SECURITY INCIDENTS!



Refer to top ten tips handset

