BIG BROTHER WATCH

Safe in Police hands?

How Police Forces suffer 10 data breaches every week and still want more of your data.

A Big Brother Watch Report

July 2016

Contents

Executive Summary

The job of the police is to protect us and in a digital society that also means protecting our data. We need to be able to trust those in authority with our personal information, unfortunately that trust is being regularly undermined.

Safe in Police hands? shows that between June 2011 and December 2015 there were at least 2,315 data breaches conducted by police staff. Over 800 members of staff accessed personal information without a policing purpose and information was inappropriately shared with third parties more than 800 times. Specific incidents show officers misusing their access to information for financial gain and passing sensitive information to members of organised crime groups.

The findings of the report reveal a number of types of data breach from improper disclosure of information, accessing police systems for non-policing purposes, inappropriate use of data and accessing data for personal reasons. Data is the driving force of society now, any of the examples highlighted pose a threat to the privacy and security of individuals.

Digital by default is the future for the country. In response to this the levels of data the police handle will increase. Whilst there have been improvements in how forces ensure data is handled correctly this report reveals there is still room for improvement. Forces must look closely at the controls in place to prevent misuse and abuse. With the potential introduction of Internet Connection Records (ICRs) as outlined in the Investigatory Powers Bill, the police will be able to access data which will offer the deepest insight possible into the personal lives of all UK citizens. Breach of such detailed information would be over and above the extent outlined in this report.

In light of this and the extended findings of our report we propose five policy recommendations. These recommendations will address concerns we have with the increased levels of data the police will have access to, they also propose more stringent methods of dealing with data breaches including a move towards error reporting and notification for the individual whose data has been breached and they ask in light of the recent vote to Brexit that the forthcoming General Data Protection Regulations are adopted despite our separation from the European Union.

Our recommendations are:

1. The introduction of custodial sentences for serious data breaches.
2. Where a serious breach is uncovered the individual should be given a criminal record.
3. The mandatory reporting of a breach that concerns a member of the public.
4. The removal of Internet Connection Records from the Investigatory Powers Bill.
5. Adoption of the General Data Protection Regulations.

These recommendations, we believe, will help give members of the public reassurance that their personal information will be kept secure, those handling it know what their responsibilities are, any misuse of it will be punished and you will be informed if your data has been breached or misused.

Key Findings

All figures for the period 1st June 2011 – 31st December 2015 unless otherwise stated

- In the past 5 years there have been 2,315 breaches in police forces, including the following:
    - 869 (38%) instances of inappropriate/unauthorised access to information
    - 877 (38%) instances of inappropriate disclosure of data to third parties.
- 25 cases involved misuse of the Police National Computer
- 1283 (55%) cases resulted in no disciplinary or formal disciplinary action being taken.
- 297 (13%) cases resulted in either a resignation or dismissal.
- 70 (3%) cases resulted in a criminal conviction or a caution.
- 258 (11%) cases resulted in either a written or verbal warning

Notable Incidents

Cleveland Police

- A special constable was dismissed for passing confidential information in relation to a detainee to a relative.

Metropolitan Police

- An officer found the name of a victim amusing and attempted to take a photo of his driving licence to send to his friend via snapchat. The officer resigned during disciplinary action.

Essex Police

- An officer has been suspended and is under investigation for abusing his position to form relationships with a number of females. It is suspected that he carried out police checks without a policing purpose.

Greater Manchester Police

- An officer informed an individual they were to be arrested. In response management action was taken.

Merseyside Police

- An officer inappropriately shared information. Allegation that officer has breached force confidentiality by attending a fellow officer's house and informing him that a sex offender lived in his road. As a result of his actions the information was passed to a third party outside the organisation

North Yorkshire Police

- Unidentified officer left paper file containing sensitive data in raided property. No action was taken as the officer could not be identified.

South Yorkshire Police

- It is alleged that whilst off duty, an officer has used mobile device to conduct a check on a vehicle. In response advice was given to the officer in question.

South Wales Police

- An officer was dismissed without notice for photographing and disseminating restricted documentation for personal gain.

Dyfed Powys Police

- An officer passed a USB device to a member of the public. It contained sensitive police information, including intelligence reports, emails and public information letters relating to crime. In response informal action was taken by the force.

Policy Recommendations

1. The introduction of custodial sentences for serious data breaches.

Existing penalties for serious data breaches are not a strong enough deterrent. Anyone found guilty of a serious breach should be subject to a potential custodial sentence.

Making the breach of Section 55 of the Data Protection Act 1998 (DPA) punishable with a custodial sentence already exists in the form of Section 77 of the Criminal Justice and Immigration Act 2008. Enacting this currently dormant piece of legislation would show that the Government is serious about safeguarding people's privacy in a data driven society.

The introduction of custodial sentences as a punishment for serious data breaches was recently supported by the Culture, Media and Sport Select Committee in their June 2016 report Cyber Security: Protection of Personal Data Online. The Committee were clear in their recommendations that "*it would be useful to have a full range of sanctions including custodial sentences*." They went on to support the calls for Section 77 and Section 78 of the Criminal Justice and Immigration Act to be enforced. The Committee are in a long line of supporters, including the Information Commissioner's Office (ICO), the Justice Select Committee, the Home Affairs Select Committee, the Science and Technology Committee, the Joint Committee on the Draft Communications Data Bill, Lord Leveson in the Leveson Review and Stephan Shakespeare in his 2013 independent review of public sector information.

2. Where a serious breach is uncovered the individual should be given a criminal record.

At present people who carry out a serious data breach are not subject to a criminal record. They could resign or be dismissed by an organisation only to seek employment elsewhere and potentially commit a similar breach. In organisations which deal with highly sensitive data, knowing the background of an employee is critical.

3. The mandatory reporting of a breach that concerns a member of the public.

We expect the police to properly protect the information they hold about us. When this fails we should have a right to know what has happened and why. Whenever a breach occurs the people affected should be informed as soon as possible – should the breach have occurred as part of an investigation, the error notification should take place within 90 days of the investigation being completed. This will allow the person to take action to mitigate the breach and seek redress.

4. The removal of Internet Connection Records from the Investigatory Powers Bill

The scale of breaches within police forces should pose major questions regarding the plans to allow police officers access to even more personal information through Internet Connection Records proposed in the IP Bill. The information the police will have access to under these powers is vast. Police forces are already struggling to keep the personal information they can access secure. It is clear that the addition of yet more data may just lead to the risk of a data breach or of misuse.

5. Adoption of the General Data Protection Regulations.

Data protection law will be a fundamental part of keeping people and businesses safe. The Information Commissioners Office have been clear that if the UK wants to trade with the Single Market "*on equal terms*" data protection standards "*would have to be equivalent to the EU's General Data Protection Regulation framework"* which will begin in 2018.

A weakening of data protection law post Brexit would put the UK at risk, in terms of trade, security and data privacy. The General Data Protection Regulations would provide a comprehensive, forward thinking approach to data protection which would the UK would be wise to adopt.

Table 1: Top 10 Police Forces

No.	Police Force	Number of Data Breaches
1	West Midlands Police	**488**
2	Surrey Police	**202**
3	Humberside Police	**168**
4	Avon and Somerset Police	**163**
5	Greater Manchester Police	**100**
6	North Yorkshire Police	**98**
7	Cheshire Constabulary	**85**
8	Dorset Police	**81**
8	Kent Police	**81**
9	Merseyside Police	**77**
10	West Mercia Constabulary	**73**

Data Protection and the Police

The Data Protection Act 1998

The Data Protection Act 1998 (DPA) governs how personal data should be gathered, stored and used responsibly. The Act defines what "*personal data*" is and presents eight data protection principles which ought to be adhered to. In short information should only ever be collected for "*legitimate purposes*", it must only ever be used for specified and lawful purposes, should not be kept longer than is necessary and should be protected from unauthorised or unlawful processing loss, destruction or damage.

Data used by the police can be acquired without the consent of the individual but the police are still required to adhere to Section 55 of the Act which makes it an offence to unlawfully obtain personal data. However, the most severe penalty which can be issued under Section 55 is a maximum fine of £500,000.

Big Brother Watch, alongside many other bodies, has long called for custodial sentences to be introduced into the Data Protection Act to address the weakness of Section 55. Custodial sentences would provide a real deterrent to those who misuse personal information. Whilst fines may appear to be adequate, there is a broad opinion that they are not strong enough to stop someone intentionally breaching the Act. Furthermore they do very little to raise awareness amongst staff about the impact a breach can have on an individual.

The ability to change this has already been legislated for. Under Section 77 of the Criminal Justice and Immigration Act 2008 Ministers can amend the DPA to give the courts the option of handing down custodial sentences of up to 2 years for the most serious offences.

Police and Personal Information

The repeated shortcomings of the police when it comes to keeping personal information secure are well publicised by both the press and in commissioner reports.

Examples of high profile cases include the failure of the British Transport Police to properly implement a system of deletion for out of date records, resulting in almost 11,000 intelligence reports not being removed and 10,000 boxes of personal information being held in archives[1].

Kent Police were fined £100,000 in March 2015 after leaving hundreds of evidence tapes and additional documents at the site of an old police station. The breach was only discovered after an officer visited the new owner of the premises and discovered them by accident. In a similar incident South Wales Police were fined £160,000 in May 2015 for losing a video recording which formed part of the evidence in a sexual abuse case. Due to a lack of training the loss went unreported for two years.

[1] BBC News, '*Poor' British Transport Police data 'risks safety'*, 19th January 2015: http://www.bbc.co.uk/news/uk-wales-30847519

In his last report the former Biometrics Commissioner painted a picture of confusion within the police when he revealed that Officers and staff routinely don't understand their responsibilities to personal information, and that data is being deleted before time or retained longer than permitted.

Police and Facial Biometrics

Most of us imagine data to be written information but images are classed as data also. The unregulated uploading of custody photos by the Metropolitan Police to the Police National Computer caused outrage in February 2015. The revelation made in the Science and Technology Committee's Biometrics report led to the then Biometrics Commissioner warning that "*hundreds of thousands*" of innocent people were now on the database[2]. The Committee called for regulation[3], but at the time of publication no moves towards regulation have been made by the Home Office and images are still being uploaded, with facial biometric methods being increasingly used at large scale public events including music festivals such as Download in Leicestershire.

Police and Data Protection

The police are under a statutory responsibility to comply with the Data Protection Act 1998. The College of Policing are clear that data protection is a "*core requirement to support effective policing*".

It is mandatory that all police and civilian staff receive a basic level of data protection training the extent of that training is not clear. Further training is provided should an individual's data responsibilities increase.

It is not a mandatory requirement for the police to report data breaches to the Information Commissioners Office. Guidance has been produced by the Information Commissioners Office to help forces decide when it may be appropriate to report an incident. In addition many forces prepare their own internal guidance and procedures for such an event.

The Investigatory Powers Bill

The Investigatory Powers Bill was laid before Parliament in March 2016, following detailed scrutiny of a draft Bill published in 2015.

The Bill as a whole will give the intelligence agencies, police and other bodies' access to greater levels of personal data and information. A number of powers such as equipment interference (better known as hacking) and the bulk collection of our communications data have been avowed. Only one new power, the collection of Internet Connection Records (ICRs) has been created.

ICRs are the retention of the websites we visit by our telecommunications services for 12 months. Not only will they list the websites a person has accessed but they will show when and what device was used as well as enabling IP address resolution – a power which many think would be possible if the UK invested in updating the current IP address technology.

---

[2] BBC News, *'Innocent people' on police photos database*, 3rd February 2015: http://www.bbc.co.uk/news/uk-31105678

[3] Science and Technology Committee, *Current and future uses of biometric data and technologies*, 25th February 2015, p. 34: http://www.publications.parliament.uk/pa/cm201415/cmselect/cmsctech/734/734.pdf

It has been argued by the Home Secretary Theresa May MP, that ICRs are the modern day equivalent of a phone bill. A description which has been roundly derided; a phone bill details the process of a one to one communication, whereas ICRs by the very nature of the internet detail one to many communications.

The websites we visit can reveal a wide range of information about use; including our health and finances, our sexuality, race, religion, age, location, family, friends and work connections.

The legislation requires the telecommunications services subject to a technical capability notice to create systems capable of retaining the Internet Connection Records for 12 months. The companies must make this information available to law enforcement agencies on request in a readable format; so even if the information has been encrypted there will be a requirement to decrypt the data so it can be read. This runs counter to the promises made by many companies including Apple and WhatsApp who encrypt users communications as standard.

Currently no other European or Commonwealth country requires the storage of web data in this form. No evidence has been presented to show why the UK is a special case or needs these powers more than any other country; the Government have expressed enthusiasm at leading the way with a new system. However they won't be the very first, a similar system was built and used in Denmark in 2007; it was abandoned after 7 years when it failed to provide any useful results. Plans to reintroduce it were scrapped because of spiralling costs[4].

The power to collect, store and for the police to subsequently seek a warrant to access our online activity would create another vulnerability to our personal data and personal lives. The failure of the Government to demonstrate the need for the power means that there are no tangible benefits to set against the negative impact the power would have on our privacy.

[4] EDRi, *Danish government postpones plans to re-introduce session logging*, 23rd March 2016: https://edri.org/danish-government-postpones-plans-to-re-introduce-session-logging/

Table 2: Full Force Breakdown

Police Force	Total Data Breaches	Number of Data Breaches	Police/Civilian	Outline of DPA breach	Action taken	Resignation	Conviction
Avon and Somerset Police	**163**	1	Information not broken down	Administrative Mistake	Information not broken down[5]		
		44		Disclosure to third party			
		98		Research person details for own benefit			
		3		Research person details for own benefit and Disclosure to a third party			
		17		Information not provided			
Bedfordshire Police	**8**	1	Officer	Police systems accessed for a non-policing purpose over a protracted period of time. Police information.	Dismissed at hearing. Criminal Caution	No	Yes
		1	Staff	Accessed police systems numerous times for a non-policing purpose. Police Information.	Gross misconduct hearing - dismissed	No	No
		1	Officer	Accessed police systems for a non-policing purpose. Police Information.	Misconduct meeting – Management advice	No	No
		1	Staff	Accessed police systems for a non-policing purpose. Police Information.	Gross misconduct meeting – Final written warning	No	No
		2	Officer	Accessed police systems for a non-policing purpose. Police	Misconduct meeting – Written Warning	No	No

[5] Response Notes: 1 police officer and 7 police staff have been dismissed, 85 police officers and 61 police staff have been disciplined internally; this includes those dismissed, six police officers and 11 police staff have resigned.

				Information.			
		1	Staff	Accessed police systems for a non-policing purpose. Police Information.	Misconduct meeting – first written warning	No	No
		1	Staff	Inappropriately revealed sensitive information to a third party. Police Information	Gross misconduct meeting – Final written warning	No	No
Cambridgeshire Constabulary	**30**	3	Staff	Use of force IT systems for a non-policing purpose	Dismissed	No	No
		1	Staff	Disclosure of police information without cause or authority	Dismissed	No	No
		3	Officer	Use of force IT systems for a non-policing purpose	Disciplinary action – Written warning	No	No
		11	Staff	Use of force IT systems for a non-policing purpose	Disciplinary action – Final Written Warning	No	No
		1	Officer	Use of force IT systems for a non-policing purpose	Disciplinary action – Final Written Warning	No	No
		2	Officer	Use of force IT systems for a non-policing purpose	Disciplinary action - Management advice	No	No
		1	Staff	Use of force IT systems for a non-policing purpose	Disciplinary action – First Written Warning	No	No
		2	Officer	Retired or resigned whilst under criminal investigation for potential breaches of Data Protection or breaches of internal procedures relating to data use.	Retired/Resigned	Yes	No
		1[6]	Staff	Information not broken down	No disciplinary action	No	No

[6] Response notes: 5 incidents related to use of IT systems for a non-policing purpose and 1 incident related to the inadvertent passing of information to a suspect of crime.

		5[7]	Officer	Information not broken down	No disciplinary action	No	No
Cheshire Constabulary	**85**	1	Police	Passed on information from Police computer records to an unauthorised person	Management action	No	No
		10	Police	Passed on information from Police investigation to an unauthorised person	No case to answer	No	No
		3	Police	Background check on a person known to them	No case to answer	No	No
		1	Police staff	Passed on information from Police investigation to an unauthorised person	Management action	No	No
		10	Police	Passed on information from Police investigation to an unauthorised person	Local resolution	No	No
		1	Police	Failed to protect confidential information	Local resolution	No	No
		2	Police staff	Passed on information from Police investigation to an unauthorised person	No case to answer	No	No
		1	Police	Passed on information from Police investigation to an unauthorised person	Management action	No	No
		1	Police	Background check on a person known to them	No case to answer	No	No
		2	Police	Background check on a person known to them	Resigned	Yes	No
		1	Police	Passed on information from Police computer records to an unauthorised person	No case to answer	No	No

[7] Response notes: 5 incidents related to use of IT systems for a non-policing purpose and 1 incident related to the inadvertent passing of information to a suspect of crime.

		1	Police staff	Posted information relating to police purposes on social media site	Dismissed	No	No
		1	Police staff	Background check on a person known to them	Written warning	No	No
		1	Police staff	Passed on information from Police computer records to an unauthorised person	Written warning	No	No
		1	Police staff	Caused the loss of personal information by sending information through a non-secure network	Written warning	No	No
		1	Police	Passed on information from Police computer records to an unauthorised person	Final written warning	No	No
		1	Police	Passed on information from Police computer records to an unauthorised person	No case to answer	No	No
		4	Police staff	Passed on information from Police investigation to an unauthorised person	Local resolution	No	No
		1	Police staff	Background check on a person known to them	Final written warning	No	No
		1	Police staff	Background check on a person known to them	Final written warning	No	No
		1	Police	Background check on a person known to them	Management action	No	No
		1	Police staff	Background check on a person known to them	Resigned	Yes	No
		1	Police	Background check on a person known to them	No case to answer	No	No
		1	Police	Passed on information from Police computer records to an	Not upheld	No	No

				unauthorised person			
		1	Police	Disclosed confidential information to a third party	Local resolution	No	No
		1	Police staff	Passed on information from Police computer records to an unauthorised person	Resigned	Yes	No
		1	Police staff	Disclosed confidential information to a third party	Local resolution	No	No
		1	Police	Disclosed confidential information to a third party	Local resolution	No	No
		1	Police	Disclosed confidential information to a third party	Upheld - management action	No	No
		2	Police	Disclosed confidential information to a third party	Local resolution	No	No
		1	Police staff	Hacked into private Facebook account	Not upheld	No	No
		1	Police staff	Disclosed confidential information to a third party	Local resolution	No	No
		3	Police	Disclosed confidential information to a third party	Not upheld	No	No
		1	Police	Obtained details from computer not for policing purpose	Not upheld	No	No
		1	Police staff	Conducted check on police systems for a non-policing purpose	Not upheld	No	No
		1	Police	Misuse of force computer systems	Not upheld	No	No
		1	Police staff	Obtained details from computer not for policing purpose	No Case to answer	No	No
		1	Police staff	Obtained details from	Resigned	Yes	No

				computer not for policing purpose			
		1	Police	Threatened to disclose police information to a third party	Not upheld	No	No
		1	Police	Disclosed confidential information to a third party	Not upheld	No	No
		1	Police	Posted personal information on social media	Local resolution	No	No
		1	Police	Disclosed confidential information to a third party	Local resolution	No	No
		1	Police	Disclosed confidential information to a third party	Not upheld	No	No
		1	Police	Posted personal information on social media	Not upheld	No	No
		1	Police	Obtained details from computer not for policing purpose	Not upheld	No	No
		1	Police	Posted personal information on social media	Management action	No	No
		1	Police	Improper information held on PNC	Not upheld	No	No
		1	Police	Disclosed confidential information to a third party	Local resolution	No	No
		1	Police	Disclosed confidential information to a third party	Not upheld	No	No
		1	Police	Passed on information from Police computer records to an unauthorised person	Local resolution	No	No
		1	Police	Disclosed confidential information to a third party	Local resolution	No	No
		1	Police	Posted personal information on social media	Local resolution	No	No

		1	Police	Disclosed confidential information to a third party	Not upheld	No	No
		1	Police	Disclosed confidential information to a third party	Local resolution	No	No
		1	Police	Disclosed confidential information to a third party	Local resolution	No	No
		1	Police staff	Disclosed confidential information to a third party	Not upheld	No	No
		1	Police	Obtained details from computer not for policing purpose	Management action	No	No
City of London Police	**4**	1	Police	Inappropriate disclosure of information regarding another officer	Disciplined internally	No	No
		1	Police	Inappropriate disclosure of information regarding another officer	Resigned during disciplinary proceedings	Yes	No
		2	Information not provided	Neither are considered section 55 offences under the Data Protection Act			
Cleveland Police	**17**	1	Special Constable	Passed confidential information to a relative in relation to detainee	Dismissed	No	No
		1	Police	Disclosed information to a third party	Resigned	Yes	No
		3	Police	Accessed information not for policing purposes	Written Warning	No	No
		1	Police	View images, no policing reason	Written Warning	No	No
		3	Police	Accessed information not for policing purposes	Resigned	Yes	No
		1	Support Staff	Accessed documents and used information contained therein	Resigned	Yes	No

		2	Support Staff	Accessed information not for policing purposes	Written Warning	No	No
		1	Police	Passed information to a member of the public	Resigned before court case was heard	Yes	No
		1	Police	Discussed cases with a member of the public	Written Warning	No	No
		1	Police	Party	Resigned	Yes	No
		1	Police	Accessed information not for policing purposes	Final Written Warning	No	No
		1	Police	Accessed information not for policing purposes	Management Action	No	No
Cumbria Constabulary	**No response**						
Derbyshire Constabulary	**47**	1	Police	Information not provided	Dismissed	No	No
		7	Police	Information not provided	Disciplined internally	No	No
		2	Civilian	Information not provided	Disciplined internally	No	No
		1	Police	Information not provided	Resigned during disciplinary	Yes	No
		2	Civilian	Information not provided	Resigned during disciplinary	Yes	No
		32	Police	Information not provided	No disciplinary action	No	No
		2	Civilian	Information not provided	No disciplinary action	No	No
Devon and Cornwall Police	**67**	2	Police	Information not provided	Convicted	No	Yes
		3	Civilian	Information not provided	Convicted	No	Yes
		3	Police	Information not provided	Dismissed	No	No
		2	Civilian	Information not provided	Dismissed	No	No
		25	Police	Information not provided	Disciplined internally	No	No
		21	Civilian	Information not provided	Disciplined internally	No	No
		3	Police	Information not provided	Resigned	Yes	No
		6	Civilian	Information not provided	Resigned	Yes	No

		1	Police	Shared information from witness statement with another witness	No disciplinary action	No	No
		1	Civilian	PCSO disclosed information about family member during enquiries	No disciplinary action	No	No
Dorset Police	**81**	4	Officer	Inappropriate access to/and or disclosure of personal data to a third party	Convicted	No	Yes
		1	Staff	Inappropriate access to/and or disclosure of personal data to a third party	Convicted	No	Yes
		3	Officer	Inappropriate access to/and or disclosure of personal data to a third party	Dismissed	No	No
		1	Staff	Inappropriate access to/and or disclosure of personal data to a third party	Dismissed	No	No
		7	Officer	Inappropriate access to/and or disclosure of personal data to a third party	Disciplined Internally	No	No
		13	Staff	Inappropriate access to/and or disclosure of personal data to a third party	Disciplined Internally	No	No
		8	Officer	Inappropriate access to/and or disclosure of personal data to a third party	Resigned during disciplinary	Yes	No
		2	Staff	Inappropriate access to/and or disclosure of personal data to a third party	Resigned during disciplinary	Yes	No
		30	Officer	Inappropriate access to/and or disclosure of personal data to a third party	No disciplinary action	No	No

		12	Staff	Inappropriate access to/and or disclosure of personal data to a third party	No disciplinary action	No	No
Durham Police	**13**	1	Civilian	Access police systems around member of OCG for non-policing purpose – no evidence of disclosure. Confidential internal report.	First written warning issued.	No	No
		1	Police	Accessed police systems for non-policing purpose. Internal reporting.	Resigned prior to facing misconduct hearing	Yes	No
		1	Police	Accessed policing systems for non-policing purpose, with suspicion that this was disclosed to suspect in criminal investigation, but not substantiated. Complaint from member of public.	Resigned prior to facing misconduct hearing	Yes	No
		1	Police	Accessed police systems for non-policing purpose, and used information to own benefit. Confidential reporting from member of public.	Resigned prior to facing misconduct hearing	Yes	No
		1	Staff	Accessed force systems and believed to share information with relative to the third persons benefit. Public complaint.	Resigned prior to facing misconduct hearing	Yes	No
		1	Staff	Accessed force systems for non-policing purpose. Confidential internal reporting.	Resigned prior to facing misconduct hearing	Yes	No
		1	Police	Disclosed information about	Management advice.	No	No

				subject to Fire Service – Inadvertent, no intent. Complaint from public.	Personal Lessons learned.		
		1	Police	Inadvertent disclosure of personal information to suspect re source of information. Complaint from public.	Management advice. Lessons.	No	No
		1	Police	Inappropriate passing of personal information to Prison Service re inmate. Complaint.	Management advice. Lessons.	No	No
		1	Staff	Inadvertent copying of email to other professional in Health Service about named. Complaint.	Management advice. Lessons.	No	No
		1	Police	Pass information to solicitor about subject – inadvertent, no intent. Complaint.	Management advice. Lessons.	No	No
		1	Police	Inaccurate disclosure of information re subject to Housing Association. Complaint.	Management advice. Lessons.	No	No
		1	Police	Disproportionate disclosure to OFSTED about subjects past history. Complaint.	Management advice. Lessons.	No	No
Dyfed Powys Police	**8**	1	Civilian	Unlawful disclosure of information to a family member. Verbal disclosure re: incident.	Written Warning	No	No
		1	Police	Unlawful disclosure of sensitive information to a member of public. Verbal disclosure re: crime.	Written Warning	No	No

		1	Police	Unlawful disclosure of information to a family member. Verbal disclosure re: crime.	Management Advice	No	No
		1	Police	Unlawful access to information on police systems in relation to a family member. Custody Record, Crime Scene Report & Case Preparation Record viewed - no data disclosed externally.	Written Warning	No	No
		1	Police	Disclosure of information to neighbour of a complainant. Officer posted a card through neighbours' door in error. The card contained data regarding an incident he had reported in relation to a third party. The information did not contain any personal data (DPA 1998) that would not already be known to the neighbours.	Management Action (informal action – not formal disciplinary action).	No	No
		1	Police	Sensitive police information passed to a member of public on a USB device. Intelligence Reports, emails, public information letters relating to crime matters.	Management Action (informal action – not formal disciplinary action).	No	No
		1	Police	Unlawful access to Force systems. Checks on police data bases in relation to a third party to be a friend of the officer.	Management Action (informal action – not formal disciplinary action).	No	No

		1	Police	Unlawful access to Force systems. Officer inappropriately accessed Force systems re: historical case whereby officer was the victim.	Management Action (informal action – not formal disciplinary action).	No	No
Essex Police[8]	**6**	1	Police	It is alleged that an officer inappropriately disclosed police information.	The officer is under suspension.	No	No
		1	Police	A complaint has been made that an officer sent inappropriate communications to a female after attending her home to deal with an incident.	A guilty plea was entered at Crown Court and a sentencing date is yet to be set.	No	Yes
		1	Police Staff	A member of police staff has accessed and viewed a large quantity of records on Essex Police System and PNC relating to their family, friends and associates.	The member of staff is under suspension. Crown Prosecution Service charging advice has been sought.	N/A	N/A
		1	Police	It is alleged that an officer accessed and disclosed police information regarding an incident involving a relative.	A gross misconduct meeting is to be held.	No	No
		1	Police	An officer is under investigation for abusing his position to form relationships with a number of females. It is also suspected that has carried out police checks	The officer is under suspension. A file has been submitted to the Crown Prosecution Service.	N/A	N/A

[8] Information obtained via the Force's quarterly reports on Complaints, Misconduct and Other Matters.

				without a policing purpose			
		1	Police and Police Staff	An officer and a member of police staff have both received a criminal caution for Data Protection Act offences.	The officer is to attend a Gross Misconduct Hearing in April 2016. The police staff member had resigned prior to the commencement of the PSD investigation.	Yes	No
Gloucestershire Constabulary	**No response**						
Greater Manchester Police	**100**	1	Officer	The officer is suspected of conducting checks for a non-policing purpose. Misuse of Force Systems. Disclosure of Information	Meeting - Written Warning	No	No
		1	Staff	Disclosed sensitive information on Facebook. Disclosure of Information.	Proven - Management Action	No	No
		1	Officer	Performed PNC checks believed to have been for own use. Misuse of PNC. Misuse of Force Systems.	Retired prior to misconduct	No	No
		1	Officer	Officer used GMP systems for own use. Misuse of Force Systems.	Meeting - Written Warning	No	No
		1	Officer	Searched GMP systems believed to be for own use. Misuse of Force Systems. Disclosure of Information.	Proven - Management Action (Advice)	No	No
		1	Officer	Obtaining and passing data. Misuse of Force Systems.	Caution/resigned prior to misconduct	Yes	No

				Disclosure of Information. Criminal conduct: Data Protection.			
		1	Officer	Allegation that a police staff accessed in relation to a personal matter. Misuse of Force Systems.	Proven - Management Action	No	No
		1	Officer	Allegation that officer downloaded body worn camera images. Misuse of Force Systems.	Meeting - Final written warning	No	No
		1	Staff	The support staff member was found to have breached data protection. Disclosure of Information.	Proven - Management Action (Advice)	No	No
		1	Officer	Investigation into allegation that the officer has sent an e-mail. Misuse of Force Systems.	Proven - Management Action (Advice)	No	No
		1	Staff	Unlawfully modified GMP data for personal gain. Misuse of Force Systems. Criminal conduct: Data Protection.	Hearing - Final written warning	No	No
		1	Officer	Alleges that officers have disclosed information. Disclosure of Information.	Proven - Management Action (Advice)	No	No
		1	Staff	Alleges a staff member is accessing GMP systems to provide information. Misuse of Force Systems. Disclosure of Information.	Resigned prior to misconduct	Yes	No
		1	Staff	Accessed police computers. Misuse of Force Systems. Criminal conduct: Data	Crown Court - Fine, costs & victim surcharge/hearing -	No	Yes

				Protection.	dismissal		
		1	Officer	PNC'd without justification. Misuse of PNC	Retired prior to misconduct	No	No
		1	Officer	Misused force systems.	Proven - Management Action (Advice)	No	No
		1	Staff	Investigation into data protection offences. Criminal conduct: Data Protection.	Caution/Hearing - dismissed	No	No
		1	Officer	Officer has accessed record for non-policing purposes. Misuse of Force Systems. Misuse of PNC.	Resigned prior to misconduct	Yes	No
		1	Staff	Disclosed operational information. Disclosure of Information.	Hearing - Written Warning	No	No
		1	Staff	Misused force computer systems. Misuse of Force Systems.	Proven - Management Action (Advice)	No	No
		1	Officer	Traced using PNC. Misuse of PNC.	Proven - Management Action (Advice)	No	No
		1	Staff	Check on the PNC a vehicle. Misuse of PNC. Criminal conduct: Data Protection.	Resigned prior to misconduct	Yes	No
		1	Officer	Officer informed… [individual] was to be arrested. Disclosure of Information.	Proven - Management Action	No	No
		1	Staff	A copy of video file sent to staff member's home email address. Misuse of Force Systems. Criminal conduct: Data Protection.	Crown Court - Not guilty/hearing - dismissed	No	No
		1	Staff	Concerns that an [officer] had accessed a FWIN. Misuse of	Proven - Management Action (Advice)	No	No

				Force Systems.			
		1	Staff	Accessing confidential GMP data for non-policing purposes. Misuse of Force Systems. Misuse of PNC.	Caution/Hearing - dismissed	No	No
		1	Staff	Data protection issues and failing to declare a notifiable association. Misuse of Force Systems.	Resigned prior to misconduct	Yes	No
		1	Officer	Officer, allowed access to passwords. Misuse of Force Systems.	Proven - Management Action (Advice)	No	No
		1	Staff	Staff member accessed FWIN for personal reasons. Misuse of Force Systems.	Proven - Management Action (Advice)	No	No
		1	Staff	Staff member accessed police systems for own purposes. Criminal conduct: Data Protection.	Magistrates Court - Fine/Hearing - Dismissed	No	No
		1	Officer	Used GMP systems to research further provide information and request action. Misuse of Force Systems.	Proven - Management Action (Advice)	No	No
		1	Staff	Conspiracy to commit misconduct in a public office. Misuse of Force Systems. Disclosure of Information.	Crown Court - Not guilty/hearing. Dismissal.	No	No
		1	Officer	Made use of the system to access police information without having a bonefide policing purpose. Misuse of Force Systems.	Proven - Management Action (Advice)	No	No

		1	Officer	Accessed for non-policing matters. Misuse of Force Systems.	Resigned	Yes	No
		1	Staff	PCSO told to have no further dealings with case, later conducted enquiries. Misuse of Force Systems.	Hearing Written Warning	No	No
		1	Officer	Made unauthorised checks on PNC. Misuse of PNC.	Crown Court - 4 Years Imprisonment/Hearing - Dismissed	No	Yes
		1	Staff	Given out information. Disclosure of Information.	Hearing Verbal Warning	No	No
		1	Officer	Accessed record. Misuse of Force Systems.	Proven - Management Action (Advice)	No	No
		1	Special	Approached a colleague and asked to PNC a vehicle. Misuse of PNC.	Proven - Management Action (Advice)	No	No
		1	Officer	Officer has accessed PNC for information. Misuse of Force Systems. Misuse of PNC.	Proven - Management Action (Advice)	No	No
		1	Officer	Copy of statement supplied [to a third party]. Disclosure of Information.	Proven - Management Action (Advice)	No	No
		1	Officer	Believes information being manufactured by an officer. Misuse of Force Systems.	Proven - Management Action	No	No
		1	Staff	Shared confidential information. Disclosure of Information.	Proven - Management Action (Advice)	No	No
		1	Officer	Misused to disprove claims. Misuse of Force Systems.	Proven - Management Action (Advice)	No	No
		1	Staff	Accessed PNC and OPUS for non-policing purposes. Misuse	Proven - Management Action (Advice)	No	No

				of Force Systems. Misuse of PNC.			
		1	Officer	Officer used GMP systems without a legitimate policing purpose. Misuse of Force Systems.	Proven - Management Action (Advice)	No	No
		1	Staff	Unlawfully modifying data on GMP systems concerning member of police staff. Misuse of Force Systems.	Hearing - dismissed	No	No
		1	Staff	Accessed records for a non-policing purpose. Misuse of Force Systems.	Proven - Management Action (Advice)	No	No
		1	Officer	Alleged use systems for other than a policing purpose. Misuse of Force Systems	Proven - Management Action (Advice)	No	No
		1	Officer	Forwarded photos of work related incidents. Misuse of Force Systems. Disclosure of Information.	Proven - Management Action (Advice)	No	No
		1	Officer	Officer is believed to have accessed GMP systems concerning member of police staff. Misuse of Force Systems.	Proven - Management Action (Advice)	No	No
		1	Officer	Officer checked the voters register and obtained details. Misuse of Force Systems.	Proven - Management Action (Advice)	No	No
		1	Officer	Officer accessing nominals. Misuse of Force Systems. Disclosure of Information.	Meeting - Final written warning	No	No
		1	Officer	Accessed GMP systems for non-policing purpose.	Meeting - Final written warning	No	No

				Disclosure of Information. Misuse of Force Systems.			
		1	Officer	Access GMP systems for a non-policing purpose. Misuse of Force Systems. Disclosure of Information. Criminal conduct: Data Protection.	Crown Court - 2 Years 9 Months Imprisonment/Hearing - Dismissed	No	Yes
		1	Officer	The officer was found to have viewed for a non-policing purpose. Misuse of Force Systems.	Proven - Management Action (Advice)	No	No
		1	Special	Accessed crime reports for non-policing purpose. Misuse of Force Systems.	Proven - Management Action (Advice)	No	No
		1	Officer	Alleges unauthorised access to GMP systems to gain personal details and disclosed to colleagues. Misuse of Force Systems.	Meeting - Final written warning	No	No
		1	Officer	Disclosed information. Disclosure of Information.	Proven - Management Action (Advice)	No	No
		1	Officer	An officer check system concerning a friend. Misuse of Force Systems.	Proven - Management Action (Advice)	No	No
		1	Staff	Member of staff accessed system without authority. Misuse of Force Systems.	Proven - Management Action (Advice)	No	No
		1	Staff	[Accessed colleagues email account]. Misuse of Force Systems	Proven - Management Action (Advice)	No	No
		1	Officer	Officer has accessed GMP records not for policing purpose. Misuse of Force	Hearing - Final Written Warning	No	No

				Systems.			
		1	Officer	Unauthorised use of police databases. Misuse of Force Systems.	Meeting - Final written warning	No	No
		1	Staff	Staff member allegedly accessed records using a GMP computer system, for non-policing purposes. Misuse of Force Systems.	Hearing - Final Written Warning	No	No
		1	Officer	Officer used a colleague's log on details to access GMP e-mail account. Misuse of Force Systems. Disclosure of Information.	Meeting - Written warning	No	No
		1	Staff	Staff member disclosed information of incident. Disclosure of Information.	Proven - Management Action	No	No
		1	Staff	Staff member shared information outside of GMP that should not be disclosed. Disclosure of Information.	Proven - Management Action (Advice)	No	No
		1	Officer	Officer has provided information concerning a case. Disclosure of Information. Misuse of Force Systems.	Proven - Management Action	No	No
		1	Officer	Accessed and divulged information. Disclosure of Information. Misuse of Force Systems.	Meeting - Written warning	No	No
		1	Officer	Using the force PNC system to locate details. Misuse of PNC.	Proven - Management Action	No	No
		1	Officer	Officer allegedly accessed	Proven - Management	No	No

				force system whilst off duty. Misuse of Force Systems.	Action		
		1	Officer	Officer has provided details to other party. Misuse of PNC. Disclosure of Information.	Meeting - Written warning	No	No
		1	Officer	Officer allegedly carried out an unauthorised PNC check using force systems. Misuse of PNC.	Proven - Management Action (Advice)	No	No
		1	Officer	Officer viewed [record] and posted comment. Disclosure of Information.	Proven - Management Action (Advice)	No	No
		1	Staff	Staff member disclosed information regarding work. Disclosure of Information.	Resigned prior to misconduct	Yes	No
		1	Staff	Officer checked OPUS. Misuse of Force Systems.	Proven - Management Action (Advice)	No	No
		1	Staff	Staff member allegedly carried out search using a force system. Misuse of Force Systems.	Proven - Management Action (Advice)	No	No
		1	Officer	Officer checked GMP systems. Disclosure of Information.	Proven - Management Action	No	No
		1	Staff	Checked FWIN and passed information. Disclosure of Information.	Hearing - Written Warning	No	No
		1	Officer	Officer had a lot of information which would not have been general knowledge. Disclosure of Information. Misuse of Force Systems.	Proven - Management Action	No	No
		1	Staff	[Accessing GMP system]. Disclosure of Information.	Proven - Management Action (Advice)	No	No

				Misuse of Force Systems.			
		1	Officer and Staff	Staff member has viewed FWIN without authority or good reason. In addition staff members failed to report this breach of data protection. Disclosure of Information. Misuse of Force Systems.	Proven - Management Action (Advice)	No	No
		1	Officer	Officer misusing GMP systems. Misuse of Force Systems.	Proven - Management Action (Advice)	No	No
		1	Staff	Member of staff accessed a PNC. Misuse of PNC.	Proven - Management Action	No	No
		2	Officer	Officer Accessed records without a policing purpose. Misuse of Force Systems.	Proven - Management Action	No	No
		1	Officer	Officer accessed GMP computer systems, none of the access was for a policing purpose. Misuse of Force Systems.	Meeting - Written Warning	No	No
		1	Officer	Officer took a photograph forwarded to colleagues. Misuse of Force Systems.	Proven - Management Action	No	No
		1	Officer	Access information for own curiosity and personal use. Misuse of Force Systems.	Proven - Management Action (Advice)	No	No
		1	Staff	Officer accessed confidential data and disclosed this information. Disclosure of Information. Misuse of Force Systems.	Resigned prior to misconduct	Yes	No
		1	Officer	Confidential documents	Proven - Management	No	No

				passed on. Disclosure of Information.	Action		
		1	Staff	Member of staff alleged to have accessed records also disclosed information. Misuse of Force Systems.	Resigned prior to misconduct	Yes	No
		1	Officer	Officer accessed police records for a non-policing reason. Misuse of Force Systems.	Proven - Management Action (Advice)	No	No
		1	Staff	Staff member accessing force systems to find out information then disclosing the information. Misuse of Force Systems. Disclosure of Information.	Proven - Management Action (Advice)	No	No
		1	Staff	Misused GMP systems. Misuse of Force Systems.	Meeting - Final written warning	No	No
		1	Officer	Officer disclosed report. Disclosure of Information.	Proven - Management Action	No	No
		1	Officer	Officer accessed a FWIN. Misuse of Force Systems.	Proven - Management Action	No	No
		1	Staff	Looking a nominals. Misuse of Force Systems.	Proven - Management Action	No	No
		1	Officer	Officer advised not to access records. It was later found had accessed record. Misuse of Force Systems.	Proven - Management Action (Advice)	No	No
Gwent Constabulary	**Refused - Cost and Time**						
Hampshire Constabulary	**Refused - Cost and Time**						
Hertfordshire	**7**	1	Police	Use of police systems for a	Disciplinary	No	No

Constabulary				non-policing purpose	proceedings - Management advice		
		6	information not provided	Information not provided	Management action	No	No
Humberside Police	**168**	1	Staff	Emailed confidential information to home computer. Police information.	Formal Misconduct. Written Warning.	No	No
		1	Police	Accessed police systems for a non-policing purpose. Police information.	Informal Misconduct. Management action.	No	No
		1	Police	Disclosure to other agency partners. Police information.	Not Upheld. NFA.	No	No
		1	Police	Accessed police systems for a non-policing purpose. Police information.	Informal Misconduct. Management action.	No	No
		1	Police	Disclosure of details of complaint's husband. Personal information.	Not Upheld. NFA.	No	No
		1	Police	Disclosure of details of a police operation to a third party. Police information.	Not Upheld. Management action.	No	No
		1	Police	Accessed police systems for a non-policing purpose. Police and personal information.	Resigned during investigation. Resigned.	Yes	No
		1	Police	Accessed police systems for a non-policing purpose. Police information.	Informal Misconduct. Management action.	No	No
		1	Police	Disclosure of information to a third party. Personal information.	Withdrawn. NFA.	No	No
		1	Police	Accessed police systems for a non-policing purpose. Police and persona information.	Formal Misconduct. Final Written Warning.	No	No
		1	Police	Use of police systems to obtain personal details. Personal information.	Withdrawn. NFA.	No	No

1	Police	Accessed police systems for a non-policing purpose. Police and personal information.	Formal Misconduct. Written warning.	No	No
1	Police	Disclosure to a third party. Personal information.	Not Upheld. NFA.	No	No
1	Police	Accessed police systems for a non-policing purpose. Police and personal information.	Formal Misconduct. Final Written Warning.	No	No
1	Police	Disclosure of bank account details. Personal information.	Dispensation by IPCC. NFA.	No	No
1	Police	Use of PNC for vehicle details. Personal information.	Not Upheld. Management action.	No	No
1	Police	Accessed police systems for a non-policing purpose. Personal information.	Withdrawn. NFA.	No	No
1	Police	Disclosure of details of police incidents. Police information.	Informal Misconduct. Management action.	No	No
1	Police	Accessed police systems for a non-policing purpose. Police information.	Not Upheld. Management action.	No	No
1	Staff	Accessed police systems for a non-policing purpose. Police information.	Not Upheld. NFA.	No	No
1	Unidentified	Disclosed information to neighbours. Personal information.	Locally Resolved. NFA.	No	No
1	Staff	Disclosed information about previous convictions. Personal information.	Not Upheld. NFA.	No	No
1	Police	Accessed police systems for a non-policing purpose. Personal information.	Formal Misconduct. Management advice.	No	No
1	Police	Accessed police systems for a non-policing purpose. Police information.	Resigned prior to hearing. Resigned.	Yes	No
1	Police	Disclosed information to a third	Locally Resolved. NFA.	No	No

		party. Personal information.			
1	Staff	Disclosed details of a traffic accident. Personal information.	Locally Resolved. NFA.	No	No
1	Police	Disclosed information to an employer. Personal information.	Not Upheld. NFA.	No	No
1	Police	Accessed police systems for a non-policing purpose. Police information.	Not Upheld. NFA.	No	No
1	Police	Improper disclosure of information. Personal information.	Withdrawn. NFA.	No	No
1	Police	Disclosure of information to neighbours. Police/Personal information.	Not Upheld. NFA.	No	No
1	Staff	Improper access and disclosure of information. Police/Personal information.	Withdrawn. NFA.	No	No
1	Police	Disclosed personal information. Personal information.	Not Upheld. NFA.	No	No
1	Police	Improper disclosure of information to employer. Personal information.	Informal Misconduct. Management action.	No	No
1	Police	Accessed police systems for a non-policing purpose. Police information.	Informal Misconduct. Management action.	No	No
1	Police	Improper disclosure of information. Personal information.	Not Upheld. NFA.	No	No
1	Staff	Improper disclosure to employer. Police information.	Locally Resolved. NFA.	No	No
1	Police	Information supplied to neighbours. Police/Personal information.	Not Upheld. NFA.	No	No
1	Police	Sent email over a non-secure network. Police/Personal information.	Informal Misconduct. Management action.	No	No

		1	Police	Improper disclosure of information. Personal information.	Locally Resolved. NFA.	No	No
		1	Police	Accessed police systems for a non-policing purpose. Police information.	Formal Misconduct. Management advice.	No	No
		1	Police	Accessed police systems for a non-policing purpose. Police information.	Formal Misconduct. Management advice.	No	No
		1	Police	Checked police systems for personal details. Personal information.	Locally Resolved. NFA.	No	No
		1	Police	Improper disclosure of information. Personal information.	Withdrawn. NFA.	No	No
		1	Police	Improper disclosure of information. Police/Personal information.	Not Upheld. NFA.	No	No
		1	Staff	Improper disclosure of information to employer. Personal information.	Locally Resolved. NFA.	No	No
		1	Police	Disclosure of previous convictions. Personal information.	Not Upheld. NFA.	No	No
		1	Police	Improper access for a non-policing purpose. Personal information.	Informal Misconduct. Management action.	No	No
		1	Police	Accessed police systems for a non-policing purpose. Personal information.	Informal Misconduct. Management action.	No	No
		1	Police	Disclosed personal information. Personal information.	Informal Misconduct. Management action.	No	No
		1	Police	Accessed police systems for a non-policing purpose. Police/Personal information.	Formal Misconduct. Final Written Warning.	No	No
		1	Staff	Improper disclosure of	Not Upheld. NFA.	No	No

		information. Personal information.			
1	Police	Improper access and disclosure of information to a third party. Police/Personal information.	Not Upheld. NFA.	No	No
1	Police	Accessed police systems for a non-policing purpose. Police information.	Not Upheld. Management action.	No	No
1	Unidentified	Accessed and disclosed information to a third party. Personal information.	Withdrawn. NFA.	No	No
1	Unidentified	Unauthorised disclosure of information to a third party. Personal information.	Withdrawn. NFA.	No	No
1	Police	Improper disclosure to a third party. Personal information.	Not Upheld. NFA.	No	No
1	Staff	Improper disclosure to a partner agency. Personal information.	Not Upheld. NFA.	No	No
1	Police	Accessed police systems for a non-policing purpose. Police information.	Formal Misconduct. Management advice.	No	No
1	Police	Improper disclosure to a third party. Police/Personal information.	Withdrawn. NFA.	No	No
1	Police	Improper access and disclosure to a third party. Personal information.	Withdrawn. NFA.	No	No
1	Police	Improper disclosure of confidential information. Personal information.	Not Upheld. NFA.	No	No
1	Police	Checks on a vehicle for a non-policing purpose. Police/Personal information.	Formal Misconduct. Not upheld.	No	No
1	Police	Accessed records of family members. Police/Personal information.	Formal Misconduct. Final Written Warning.	No	No

		1	Police	Accessed information of associates for non-policing purposes. Police/Personal information.	Formal Misconduct. Written Warning.	No	No
		1	Staff	Improper disclosure of information about a CCTV camera. Police information.	Locally Resolved. NFA.	No	No
		1	Police	Improper disclosure of medical information to a third party. Personal information.	Locally Resolved. NFA.	No	No
		1	Police	Accessed and disclosed records of associates. Police/Personal information.	Formal Misconduct. Final Written Warning.	No	No
		1	Police	Improper disclosure of information to a partner agency. Personal information.	Withdrawn. NFA.	No	No
		1	Staff	Inappropriate disclosure of information to employers. Police/Personal information.	Withdrawn. NFA.	No	No
		1	Police	Improper disclosure of information to the press. Police/Personal information.	Withdrawn. NFA.	No	No
		1	Police	Improper access for a non-policing purpose. Police/Personal information.	Formal Misconduct. Written Warning.	No	No
		1	Police	Improper disclosure of information re a DV incident. Personal information.	Locally Resolved. NFA.	No	No
		1	Police	Added information to a database. Personal information.	Not Upheld. NFA.	No	No
		1	Staff	Improper disclosure of information. Police information.	Not Upheld. NFA.	No	No
		1	Police	Improper disclosure of information to a school. Personal information.	Not Upheld. NFA.	No	No
		1	Police	Accessed information of	Formal Misconduct.	No	No

		associates for non-policing purposes. Police/Personal information.	Management advice.		
1	Police	Disclosure of information. Personal information.	Locally Resolved. Words of advice.	No	No
1	Police	Improper disclosure of information. Police/Personal information.	Not Upheld. NFA.	No	No
1	Police	Improper disclosure of information. Police/Personal information.	Locally Resolved. NFA.	No	No
1	Police	Improper access and disclosure. Police information.	Resigned prior to charges. Resigned.	Yes	No
1	Unidentified	Inappropriate disclosure of information to finance company. Personal information.	Locally Resolved. NFA.	No	No
1	Police	Accessed for a non-policing purpose and improper disclosure. Police/Personal information.	Informal Misconduct. Management action.	No	No
1	Staff	Disclosure to a third party. Personal information.	Resigned during investigation. Resigned.	Yes	No
1	Police	Improper disclosure of information. Police information.	Not Upheld. NFA.	No	No
1	Police	Disclosed details of a colleague. Personal information.	Not Upheld. NFA.	No	No
1	Staff	Accessed police systems for a non-policing purpose. Police/Personal information.	Withdrawn. NFA.	No	No
1	Police	Accessed police systems for a non-policing purpose/improper disclosure. Personal information.	Not Upheld. NFA.	No	No
1	Police	Accessed police systems for a non-policing purpose. Police/Personal information.	Formal Misconduct. Final Written Warning.	No	No
1	Staff	Improper disclosure to family members. Police/Personal	Locally Resolved. NFA.	No	No

		information.			
1	Staff	Inappropriate access and disclosure. Police/Personal information.	Not Upheld. NFA.	No	No
1	Staff	Accessed police systems for a non-policing purpose. Police/Personal information.	Not Upheld	No	No
1	Police	Improper disclosure of information to an offender. Police information.	Locally Resolved. NFA.	No	No
1	Police	Inappropriate access and disclosure to family members. Personal information.	Not Upheld. NFA.	No	No
1	Unidentified	Information supplied to a forum. Police/Personal information.	Withdrawn. NFA	No	No
1	Police	Improper disclosure of information to a third party. Personal information.	Locally Resolved. NFA.	No	No
1	Staff	Improper disclosure to a third party. Police/Personal information.	Locally Resolved. NFA.	No	No
1	Police	Improper access and copying of data. Personal information.	Not Upheld. NFA.	No	No
1	Staff	Improper disclosure of information to a third party. Police/Personal information	Locally Resolved. NFA.	No	No
1	Staff	Improper access for a non-policing purpose. Police information.	Formal Misconduct. Verbal Warning.	No	No
1	Police	Improper disclosure of information to a third party. Personal information.	Locally Resolved. NFA.	No	No
1	Police	Improper access for a non-policing purpose. Police/Personal information.	Informal Misconduct. Management action.	No	No

		1	Staff	Improper disclosure of information to employer. Police/Personal information.	Locally Resolved. NFA.	No	No
		1	Police	Improper disclosure of information to a council employee. Personal information.	Locally Resolved. NFA.	No	No
		1	Police	Disclosure of information via a letter. Police/Personal information.	Not Upheld. NFA.	No	No
		1	Police	Sent emails to an insecure email address. Personal information.	Formal Misconduct. Written warning.	No	No
		1	Staff	Improper disclosure of information to council. Personal information.	Not Upheld. NFA.	No	No
		1	Staff	Accessed policing systems for non-policing purposes. Police information.	Formal Misconduct. Written Warning.	No	No
		1	Staff	Accessed policing systems for non-policing purposes. Police information.	Formal Misconduct. Written Warning.	No	No
		1	Police	Accessed policing systems for non-policing purposes. Police information.	Not Upheld. NFA.	No	No
		1	Police	Inappropriate disclosure of information via Facebook. Police information.	Disapplied. NFA.	No	No
		1	Police	Accessed police systems for a non-policing purpose. Police information.	Not Upheld. NFA.	No	No
		1	Staff	Accessed police systems for a non-policing purpose. Police information.	Not Upheld. NFA.	No	No
		1	Staff	Unauthorised access and improper disclosure of information to a third party. Personal information.	Not Upheld. NFA.	No	No

1	Unidentified	Improper disclosure of information to a third party. Police/Personal information.	Withdrawn. NFA.	No	No
1	Staff	Accessed information for non-policing purposes. Police/Personal information.	Formal Misconduct. Written Warning.	No	No
1	Staff	Improper disclosure of information. Personal information.	Locally Resolved. Management action.	No	No
1	Unidentified	Improper disclosure of information to an employer. Police/Personal information.	Withdrawn. NFA.	No	No
1	Police	Improper disclosure of information. Personal information.	Locally Resolved. NFA.	No	No
1	Police	Improper disclosure of information to a third party. Police/Personal information.	Withdrawn. NFA.	No	No
1	Police	Accessed information for non-policing purposes. Police information.	Informal Misconduct. Management action.	No	No
1	Police	Accessed information for a non-policing purpose. Police information.	Informal Misconduct. Management action.	No	No
1	Staff	Improper access and disclosure to a third party. Personal information.	Resigned during investigation. NFA.	No	No
1	Police	Accessed information for a non-policing purpose. Personal information.	Not Upheld. NFA.	No	No
1	Staff	Improper disclosure of information. Personal information.	Locally Resolved. NFA.	No	No
1	Police	Accessed information for a non-policing purpose. Police information.	Not Upheld. NFA.	No	No

		1	Staff	Accessed information for a non-policing purpose. Police information.	Formal Misconduct. Written warning.	No	No
		1	Staff	Improper access and disclosure to a partner agency. Police/Personal information.	Locally Resolved. NFA.	No	No
		1	staff	Accessed information for a non-policing purpose. Police/Personal information.	Formal Misconduct. Written warning.	No	No
		1	Police	Accessed information for a non-policing purpose. Police/Personal information.	Not Upheld. NFA.	No	No
		1	Staff	Accessed information for a non-policing purpose. Police/Personal information.	Formal Misconduct. Verbal Warning.	No	No
		1	Police	Improper disclosure of information to the council. Police information.	Locally Resolved. NFA.	No	No
		1	Police	Accessed information for a non-policing purpose. Police/Personal information.	Formal Misconduct. Final Written Warning.	No	No
		1	Police	Improper disclosure of information. Police information.	Not Upheld. NFA.	No	No
		1	Police	Improper disclosure of information to the NHS. Police/Personal information.	Not Upheld. NFA.	No	No
		1	Police	Improper disclosure of information to a third party. Personal information.	Locally Resolved. NFA.	No	No
		1	Staff	Improper disclosure of information. Police/Personal information.	Not Upheld. NFA.	No	No
		1	Police	Improper disclosure of information to a third party. Personal information.	Locally Resolved. NFA.	No	No
		1	Police	Accessed information for a non-	Not Upheld. NFA.	No	No

		policing purpose. Police/Personal information.			
1	Police	Accessed information for a non-policing purpose. Police information.	Not Upheld. NFA.	No	No
1	Police	Improper disclosure of information to a prison inmate. Police information.	Not Upheld. NFA.	No	No
1	Police	Improper disclosure of information about an offender. Police information.	Not Upheld. NFA.	No	No
1	Unidentified	Disclosure of incorrect information to other agencies. Police/Personal information.	Not Upheld. NFA.	No	No
1	Staff	Accessed information for a non-policing purpose. Police/Personal information.	Formal Misconduct. Verbal Warning.	No	No
1	Staff	Improper disclosure of information to a local authority. Personal information.	Not Upheld. NFA.	No	No
1	Police	Accessed information for a non-policing purpose. Police/Personal information.	Not Upheld. NFA.	No	No
1	Police	Improper disclosure of information. Police information.	Locally Resolved. NFA.	No	No
1	Police	Inappropriate access and disclosure of information for personal benefit. Police/Personal information.	Informal Misconduct. Management action.	No	No
1	Staff	Personal information.	Withdrawn. NFA.	No	No
1	Police	Improper disclosure of information during a court case. Personal information.	Upheld. NFA. CPS had released the information.	No	No
1	Police	Accessed information for a non-policing purpose. Police/Personal information.	Resigned prior to misconduct. NFA.	Yes	No

		1	VOLUNTEER	Accessed information for a non-policing purpose. Police/Personal information.	VOLUNTEER. NFA	No	No
		1	Police	Accessed information for a non-policing purpose. Police/Personal information.	Formal Misconduct. Written warning.	No	No
		1	Police	Improper disclosure of witness information. Personal information.	Locally Resolved. NFA.	No	No
		1	Police	Improper disclosure of information. Personal information.	Not Upheld. NFA.	No	No
		1	Police	Improper access and disclosure of information. Personal information.	Locally Resolved. NFA.	No	No
		1	Staff	Police information.	Not Upheld. NFA.	No	No
		1	Unidentified	Improper disclosure of information to a partner agency. Police information.	Not Upheld. NFA.	No	No
		1	Police	Improper disclosure of information at a workplace. Police/Personal information.	Locally Resolved. NFA.	No	No
		1	Unidentified	Improper disclosure of information re address. Personal information.	Locally Resolved. NFA.	No	No
		1	Police	Improper disclosure of information at Court. Personal information.	Locally Resolved. NFA.	No	No
		1	Police	Accessed information for a non-policing purpose. Police/Personal information.	Formal Misconduct. Written Warning.	No	No
		1	Police	Improper disclosure of information. Police/Personal information.	Locally Resolved. NFA.	No	No
		1	Staff	Accessed information for non-policing purpose. Police	Not Upheld. Policy re-reinforced.	No	No

				information.			
		1	Staff	Accessed information for non-policing purpose. Police/Personal information.	Formal Misconduct. Verbal Warning.	No	No
		1	Staff	Accessed information for non-policing purpose. Police/Personal information.	Not Upheld. NFA.	No	No
		1	Police	Accessed information for non-policing purpose. Police/Personal information.	Informal Misconduct. Management action. Policy re-enforced.	No	No
		1	Staff	Accessed a police log for non-policing purpose. Police information.	Not Upheld. NFA.	No	No
		1	Staff	Accessed information for a non-policing purpose. Police/Personal information.	Formal Misconduct. Written warning.	No	No
Kent Police	**81**	2	Police Officer	Records Accessed	Management Action	No	No
		19	Police Officer	Unauthorised Check	Management Action	No	No
		1	Police Officer	Unauthorised Check	Formal Action - Hearing	No	Yes
		3	Police Officer	Unauthorised Check	Resigned	Yes	No
		1	Police Officer	Computer Misuse	Resigned	Yes	No
		2	Police Staff	Inappropriate Use	Resigned	Yes	No
		2	Police Staff	Inappropriate Use	Final Written Warning	No	No
		4	Police Officer	Improper Disclosure	Resigned	Yes	No
		6	Police Officer	Unauthorised Check	No Action	No	No
		2	Police Officer	Unauthorised Check	Dismissed	No	Yes
		2	Police Staff	Improper Disclosure	Resigned	Yes	No
		9	Police Officer	Improper Disclosure	Management Action	No	No
		2	Police Staff	Improper Disclosure	Management Action	No	No
		3	Police Officer	Unauthorised Check	Management Advice	No	No
		3	Police Officer	Inappropriate Use	Management Action	No	No
		2	Police Officer	Unauthorised Check	Written Warning	No	No

		2	Police Officer	Inappropriate Use	No Action	No	No
		1	Police Staff	Unauthorised Check	Final Written Warning	No	No
		2	Police Staff	Improper Disclosure	No Action	No	No
		1	Police Staff	Improper Disclosure	Dismissed	No	Yes
		3	Police Officer	Unauthorised Check	Final Written Warning	No	No
		2	Police Staff	Unauthorised Check	No Action	No	No
		1	Special Constable	Unauthorised Check	No Action	No	No
		2	Special Constable	Unauthorised Check	Resigned	Yes	No
		1	Police Officer	Unauthorised Check	Dismissed	No	Yes
		1	Special Constable	Improper Disclosure	Resigned	Yes	No
		1	Other Police Staff	Improper Disclosure	Dismissed	No	Yes
		1	Police Officer	Improper Disclosure	No Action	No	No
Lancashire Constabulary	**16**	1	Civilian	Inappropriately shared victim information with a third party	Convicted	No	Yes
		1	Civilian	Inappropriate use of force systems	Dismissed	No	No
		2	Police	Inappropriate use of force systems	Disciplined Internally	No	No
		1	Police	Inappropriate use of force systems and inappropriately sharing information with a third party	Disciplined Internally	No	No
		1	Police	Inappropriately sharing information with a third party	Disciplined Internally	No	No
		1	Civilian	Inappropriately sharing information with a third party	Disciplined Internally	No	No
		1	Civilian	Not storing confidential documentation safely and	Disciplined Internally	No	No

				securely.			
		2	Civilian	Inappropriate use of force systems	Disciplined Internally	No	No
		1	Civilian	Inappropriate use of force systems and inappropriately sharing information with a third party	Disciplined Internally	No	No
		2	Police	Inappropriately sharing information with a third party.	Resigned during disciplinary process	Yes	No
		1	Civilian	Inappropriate use of force systems, potential disclosure of information.	Resigned during disciplinary process	Yes	No
		2	Civilian	Inappropriately sharing information with a third party.	Resigned during disciplinary process	Yes	No
Leicestershire Constabulary	**1**	1	Staff	5 charges relating to inappropriate browsing of systems and led to the magistrates convicting the individual.	Convicted and subsequently resigned	Yes	Yes
Lincolnshire Police	**Refused - Cost and Time**						
Merseyside Police	**77**	1	Police	Inappropriate use of force systems. Officer has conducted numerous dubious checks on Force systems in relation to herself and others.	Resigned and convicted	Yes	Yes
		1	Staff	Inappropriate use of force systems. Officer has multiple questionable checks. They are questionable in that they focus on his surname and one street.	No Case to Answer	No	No

		1	Police	Inappropriate use of force systems. Audit checks obtained have identified officer as having conducted questionable checks on the force systems.	No Case to Answer	No	No
		1	Police	Inappropriate use of force systems. Systems audit conducted on officer after he reported an association to PSD. Audit reveals that he has on a couple of occasions examined 2 crime files on Niche where there was an off duty victim and also searched for another person with his surname.	Officer to be provided with advice and training	No	No
		1	Police	Inappropriately shared information. Internal report submitted outlining that the officer has disclosed information about a surveillance operation she was involved in to a colleague within the Violent Offender Management Unit (VOMU), when she was explicitly asked not to.	Final written warning	No	No
		1	Staff	Inappropriate use of force systems. As a result of an intelligence report by an officer in relation to criminal	Advice and action plan given	No	No

				activity by a relative of his partner, Force systems checks were done which disclosed some inappropriate use of systems.			
		1	Police	Inappropriate use of force systems. Officer seeks permission to have access to his wife's email account whilst she is off sick to monitor responses re a joint presentation they are working on. Permission is refused and so officer then obtains wife's password and delegates her email account to him. The delegation was removed before he accessed her actual email account.	Advice provided	No	No
		1	Police	Inappropriate use of force systems. A complaint was made alleging that officer accessed Force Systems and shared the information outside of the organisation. As part of that investigation the ACU have done an audit on officer's use of Force Systems; as a result of that audit, questionable checks have been identified unconnected to the complaint matters. It is alleged that the	Advice provided	No	No

				checks were not for a policing purpose as they relate to the officer's family and individuals/locations that are known to the officer but are outside the Police organisation and its business.			
		1	Staff	Inappropriate use of force systems. Employee completed a search on systems on behalf of her colleague. Employee immediately reported the matter to a supervisor and both have submitted formal reports re their actions.	Management action	No	No
		1	Staff	Inappropriate use of force systems. Employee's daughter was a vulnerable MFH. She was not reported but employee used Force systems to identify an address connected to their daughter. On arriving at the address she was not there and so asked a colleague to conduct a further search which she did.	Management action	No	No
		1	Police	Inappropriately shared information. It is alleged that officer became aware his daughter had disclosed confidential information to her mother, who had made further disclosures and he	Management action	No	No

				failed to report the matter in an appropriate manner.			
		1	Staff	Inappropriate use of force systems and sharing information. Employee has received a test message from a friend enquiring about an incident in the St Helens area. She has responded by saying that she would have a look at the log when next on duty. When next on duty she examined the incident logs and then sent a number of text messages to her friend providing her with information about the incident.	Resigned	Yes	No
		1	Police	Inappropriately shared information. Allegation that officer has breached force confidentiality by attending a fellow officer's house and informing him that a sex offender lived in his road. As a result of his actions the information was passed to a third party outside the organisation.	Written warning	No	No

		2	Police	Inappropriately shared information. It is alleged the officer was involved in the disclosure of confidential information when not in the proper course of police duties regarding the movement of a Juvenile from GMP to the Merseyside area.	Management action	No	No
		1	Police	Inappropriate use of force systems. Questionable system checks require investigation. There is no suggestion that this information has been for a third party.	No Case to Answer	No	No
		1	Staff	Inappropriate use of force systems. Audit check revealed a number of inappropriate checks in relation to their extended family.	Dismissed	No	No
		1	Police	Inappropriate use of force systems. Audit checks show the officer may have carried out inappropriate system checks. Officer has viewed briefing sheet where he resides 3 times more often than where he works and has carried out checks on his name.	Management action	No	No
		1	Police	Inappropriate use of force systems. Audit checks show that the officer has carried out	Management action	No	No

				a number of system checks on and around current and previous address and entered crime files.			
		1	Police	Inappropriate use of force systems. Allegation officer disclosed information from police systems to his friend during a civil dispute. Checks did not confirm this allegation, but did identify historic checks in relation to his family.	No Case to Answer	No	No
		2	Police	Inappropriate use of force systems. Audit checks have identified a number of questionable force system checks.	No Case to Answer	No	No
		1	Police	Inappropriate use of force systems. Audit checks have identified a number of questionable force system checks.	Resigned	Yes	No
		1	Staff	Inappropriate use of force systems. ACU systems audit has identified a large number of system checks between 2007-2012 that do not appear to be for a policing purpose.	Resigned	Yes	No
		1	Police	Inappropriate use of force systems. Allegation that the officer has 'checked out' a black 2-door BMW motor vehicle given to his sister by	No Case to Answer	No	No

				her ex-boyfriend using police systems.			
		1	Police	Inappropriate use of force systems. Accessing force systems.	Resigned	Yes	No
		1	Staff	Inappropriate use of force systems. On 20/09/12 maintenance on the Merseyside Police Team Drive Server allowed access to secure team drive folders to unauthorised staff. Employee has accessed a number of sensitive team drive folders and copied this material to his personal computer desktop and then onto a memory stick.	Dismissed	No	No
		1	Staff	Inappropriate use of force systems. On Thursday 20/9/12 maintenance on the Merseyside Police Team Drive Server allowed access to secure team drive folders to unauthorised staff. On 20/9/12 employee has accessed a team drive and viewed a word document.	Written warning and advice given	No	No
		1	Staff	Inappropriate use of force systems. Computer Misuse, questionable system checks relating to officer, her address, daughter and daughters address and male	Dismissed	No	No

				believed to be her son, who is involved in drug supply.			
		1	Police	Inappropriate use of force systems. Audit check revealed a large number of inappropriate checks. Officer was summoned for 14 offences contrary to the DPA 1998 and 9 offences contrary to the Computer Misuse Act 1990 and following a full trial at LCM Court were convicted in relation to all matters.	Dismissed and convicted	No	Yes
		1	Police	Inappropriate use of force systems. Officer arrested for assault on partner's daughter during a domestic argument. Suggestion they may have used Forced systems to check out the partner.	Resigned and cautioned	Yes	No
		1	Staff	Inappropriate use of force systems. ACU audit suggests staff member has inappropriately accessed a niche file and may have disclosed this information.	No Case to Answer	No	No
		1	Staff	Inappropriate use of force systems. Audit highlights a number of inappropriate system checks for a non-policing purpose. These appear to include family members, vehicles	Dismissed and convicted	No	Yes

				associated to her and custody records. Officer pleaded guilty at LCC to 12 offences contrary to DPA 1998 and 1 offence contrary to the Computer Misuse Act 1990.			
		1	Staff	Password security. Whilst a member of his staff was waiting for IT system access, this employee has disclosed his log on and password details to her so she can access force systems.	Advice given	No	No
		1	Police	Inappropriate use of force systems. Allegation officer has carried out checks on vehicles in his mother's street.	No Case to Answer	No	No
		1	Police	Inappropriate use of force systems. Officer obtained personal data from Merseyside Police computer systems in respect of an associate.	Dismissed	No	No
		1	Staff	Inappropriate use of force systems. Request made on 21/02/13 to resume access to Force IT systems. Audit of computer usage shows 300 questionable checks relating to searching on addresses and names linked to her / family.	Resigned and convicted	Yes	Yes

		1	Police	Inappropriate use of force systems. Officer's partner was arrested for a number of offences whilst driving the officer's car. As a result of the arrest, the officer was required by her supervision to complete a Notifiable Association report. In the report, the officer admits researching her partner's former girlfriend on force systems. Further system audit has identified that the officer has conducted further DPA checks on another previous partner.	Resigned and convicted	Yes	Yes
		1	Police	Inappropriate use of force systems. Officer enters and updates storm log relating to TFMV in different BCU. Complainant has same name as officer.	No Case to Answer	No	No
		1	Police	Inappropriately shared information. Officer has provided information in a 104 regarding an incident she was involved in. She has disclosed that she potentially breached the DPA by providing information to a member of the public.	Advice and training provided	No	No

		1	Police	Inappropriate use of force systems. Research has indicated that the officer has carried out systems enquiries on a male in custody that cannot be accounted for, at this stage. If not for a policing purpose this would amount to a DPA criminal offence and a breach under honesty and integrity.	No Case to Answer	No	No
		1	Police	Inappropriately shared information. It has been suggested that officer has updated DV victim regarding on-going criminal investigations via Facebook.	Resigned and convicted	Yes	Yes
		1	Police	Inappropriate use of force systems. Misuse of force systems identified during vetting enquiry. Officer received final written warning 8.2.11 for similar offence. Limited checks but relates to self, home address and current partner.	Resigned and convicted	Yes	Yes
		1	Police	Inappropriate use of force systems. Evidence of questionable checks on force systems relating to premises controlled by officer.	No Case to Answer	No	No
		1	Staff	Inappropriately shared information. It is alleged	Dismissed	No	No

				employee without authority or permission has disclosed confidential police information to a senior press officer, employed by Liverpool Daily Post and Echo.			
		1	Staff	Inappropriate use of force systems. Employee has been convicted of a criminal offence under the Data Protection Act 1998, in respect of the unauthorised police systems checks on his home address.	Dismissed and convicted	No	Yes
		1	Police	Inappropriate use of force systems. Officer was convicted of a criminal offence that contravened the DPA 1998. Between 17th March 2011 and 10th May 2011, knowingly and without the consent of the data controller, unlawfully obtained personal data held on police computer systems.	Dismissed and convicted	No	Yes
		1	Police	Inappropriate use of force systems. Questionable checks by officer on force systems that are suspected to be DPA criminal offences.	Dismissed and convicted	No	Yes
		1	Police	Inappropriate use of force systems. It is alleged that the officer has breached force	No Case to Answer	No	No

				policy by using various force computer systems to conduct checks that were not for a policing purpose.			
		1	Staff	Inappropriate use of force systems. It is alleged that on 16 separate occasions between 3/2/10 and 2/9/13 employee used Merseyside Police force systems to conduct unauthorised checks on his personal vehicle including the previous registered keeper. He also conducted unauthorised checks on his own, his sisters' and neighbour's addresses. None of these checks were conducted for official police business.	Resigned	Yes	No
		1	Police	Inappropriate use of force systems. Case originates from an MFH enquiry that is linked to a relative of the officer. Her conduct surrounding this issue caused sufficient concern as to merit a report to PSD. As a result of this an ACU audit was conducted which has highlighted possible DPA offences.	No Case to Answer	No	No
		1	Police	Inappropriate use of force systems. Officer on career	Resigned	Yes	No

				break falsely claims to be on duty to access information.			
		1	Staff	Inappropriate use of force systems. ACU audit has revealed systems checks relating to the case in which the member of staff was the alleged offender.	Resigned and convicted	Yes	Yes
		1	Police	Inappropriate use of force systems. Police Inappropriate use of force systems It is alleged that the officer has conducted checks on Merseyside Police Force systems which were not for a policing purpose.	Dismissed and convicted	No	Yes
		1	Police	Inappropriate use of force systems. Off duty officer is victim of a theft of motor cycle. He is a witness in the case. The officer has then investigated his own crime, seizing and viewing CCTV, requesting ANPR checks and updating the Enquiry Log.	Management Action	No	No
		1	Police	Inappropriate use of force systems. It is alleged officer has conducted a number of questionable checks and they were not completed for a policing purpose.	Written warning	No	No

		1	Staff	Inappropriate use of force systems. The allegation is that between 27th September 2008 and 6th December 2013 employee consistently misused Merseyside Police computer systems to research information for reasons other than for a Policing purpose.	Dismissed	No	No
		1	Staff	Inappropriate use of force systems. Audit of computer use shows that police staff member has made checks on her home address, the address of her neighbour and other checks in the vicinity of her home address. Checks do not appear to be for a policing purpose.	Resigned and convicted	Yes	Yes
		1	Police	Inappropriate use of force systems. Audit has revealed that officer has conducted 5 questionable checks on her sister between 2007 and 2010.	Written warning	No	No
		1	Staff	Inappropriate use of force systems. Audit has revealed that officer has conducted questionable checks on her ex-partner, herself and a male neighbour. She has accessed crime files relating to her ex-partner and herself. Checks	Resigned	Yes	No

				conducted between 2009-2011.			
		1	Staff	Inappropriate use of force systems. Audit has revealed that member of police staff has conducted a check on her husband. Also a check on her sister's address regarding a male linked to the same address. Checks not believed to be for a policing purpose.	Management action	No	No
		1	Police	Inappropriate use of force systems. ACU audit has revealed that member of staff has made numerous systems' checks on her cousin and her cousin's son.	Advice given	No	No
		1	Staff	PCSO views incident log during normal duties, which is from her neighbour and relates to a complaint against her daughter. Later that same day PCSO admits to carrying out a check on her neighbour and also wrote down the details from the incident log she viewed and informed her own partner, which appear for personal reasons.	Final written warning	No	No
		1	Police	Inappropriate use of force systems. Complainant (partner of officer's ex-wife)	No Case to Answer	No	No

				suspects officer may have conducted an unauthorised check on PNC.			
		1	Police	Inappropriate use of force systems. Complainant suspects an officer who is his current partner's ex-husband may have conducted an unauthorised check on PNC. This officer was in the vehicle at the time of the stop check and audit checks show he searched for the vehicle.	Management action	No	No
		1	Police	Inappropriate use of force systems. Suggestion that officer has accessed force systems to look at duties of another officer who he believes is having an affair with his wife.	Meeting - Not proven	No	No
		1	Police	Officer is alleged to be in an inappropriate relationship with members of an OCG and to have passed information from the force systems to the OCG in return for payment.	Dismissed and convicted	No	No
		1	Police	Inappropriate use of force systems. It is alleged that between 3rd August 2011 and 25th September 2013 officer conducted numerous checks using Merseyside Police Systems relating to her family	Dismissed	No	No

				and their partners. It is alleged that this was not a policing purpose.			
		1	Police	Inappropriately use of force systems. Enquiries have highlighted officer has historically interrogated Force Systems in connection with the street he resides. No evidence of disclosure and appear to be 'curiosity' checks.	Management advice and training	No	No
		1	Police	Inappropriate use of force systems. It is alleged officer has conducted a number of questionable checks and they were not completed for a policing purpose.	Management action	No	No
		1	Police	Inappropriate use of force systems. On Fri 19/12/14 on 2 separate occasions you misused force systems and interrogated a Niche file related to a serious case.	Management Advice	No	No
		1	Staff	Inappropriate use of force systems. Officer self discloses that he has accessed a storm log in relation to a family matter. In making an assessment of this matter I have considered.	Management advice and training	No	No

		1	Police	Inappropriate use of force systems. An audit has been conducted around use of Force systems. This exercise has identified a number of Niche based enquiries, as well others relating to QAS, which do not appear to be for a legitimate policing purpose. The enquiries span from 2008 through to December 2014 and the nature of them appear to involve family members and also a series of enquiries regarding a nominal who is believed to be in a relationship with the officer's niece.	No Case to Answer	No	No
		1	Police	Inappropriate use of force systems. Audit has identified officer has conducted historical checks on Force systems regarding his wife being a victim of crime and his step daughter being arrested.	Management Advice	No	No
		1	Staff	Inappropriate use of force systems. Employee appears to have accessed a Niche record and viewed the content. He has then sent the implicated officer an email alerting the officer to the allegation and	Management Advice	No	No

				also that PSD have been informed.			
		1	Staff	Inappropriate use of force systems. An ACU audit has identified that employee has conducted an enquiry on Force systems regarding a male who he is involved in a personal dispute.	Resigned	Yes	No
		1	Police	Inappropriate use of force systems. Officer has come on duty and accessed Niche to research if her husband, who she is concerned for due to his serious medical issues, had been arrested. YP accesses her husband's Niche record and then alerts her supervisor to this unauthorised access. This has been reported to PSD.	Management Action	No	No
Metropolitan Police[9]	**39**	1	Officer	The officer has provided false details concerning the manner of driving and false details concerning her identity to cause inconvenience to an acquaintance. Data	Conviction	No	Yes

[9] Response notes that: "*The MPS has a flag under which alleged breaches of the Data Protection Act are recorded. This flag is used by members of staff when they perceive that a Data Protection Act breach has taken place. I further explained that it can be seen by reading the allegation summary column, that a number of the recorded breaches are not, in fact, breaches of the Data Protection Act 1998*." The response further notes that a breach, as summarised by the member of staff recording the allegation may not be representative of the actual breach as proven in a criminal court or a misconduct hearing.

				Protection Breach			
		1	Officer	Officer conducted PNC & MDT check of a vehicle and also a name check on original informants husband. - Between ****** 2011 and ******* 2011 at within the jurisdiction of the *****, without the consent of the data controller, knowingly or recklessly disclosed personal data Contrary to sections 55(3) and 60(2) of the Data Protection Act 1998.	Conviction	No	Yes
		1	Officer	OPERATION ******** - Between ******* 2005 and ********** 2010 conducted in excess of 30 unauthorised searches on MPS Intelligence and Crime recording indices	Conviction	No	Yes
		1	Officer	It is alleged that officer knowingly or recklessly, without the consent of the data controller, obtained or disclosed personal data or the information contained in personal data, contained within MPS data systems without an authorised reason.	Conviction	No	Yes
		1	Officer	Officer is believed to be passing intelligence to two	Conviction	No	Yes

				known drug dealers/users			
		1	Officer	Used MPS communications systems to pass information obtained from MPS databases to third parties outside the MPS	Conviction	No	Yes
		1	Officer	Operation ********* - Misuse of MPS databases	Conviction	No	Yes
		1	Officer	Complainant states that in **** an officer had informed her parents without her permission or knowledge that she had moved to ********** and later again that her daughter had been taken into care. Complainant did not wish these details to be divulged to her family and feels this is a breach of the data protection act.	Disciplined internally	No	No
		1	Officer	The complainant states the officer Breached Data Protection Act.	Disciplined internally	No	No
		1	Officer	The officer cited has breached data protection by sending an email using another colleagues computer who had left his desk briefly and had neglected to log off his computer. The email was sent to a senior officer and although not abusive was flippant in nature poking fun at another senior	Disciplined internally	No	No

				officer. The officer cited has come forward admitting to doing this.			
		1	Officer	Complainant states that when distributing missing person posters, police allowed for private information such as the persons address, the fact she carries money and is an alcoholic, to be shown on said poster	Disciplined internally	No	No
		1	Officer	Officer misused Met Police computer systems to submit data protection act requests for a ********** Police investigation. He had no need or authority to make these requests. He requested the resulting information be copied to him without good reason or authority	Disciplined internally	No	No
		1	Officer	The complainant alleges that the officer has unlawfully obtained both his and his relatives personal details.	Disciplined internally	No	No
		1	Officer	Complainant states officer revealed matters of a very embarrassing and unproven nature to his parents.	Disciplined internally	No	No

		1	Officer	The complainant states that the officer told his father the details of his bail and states that this is a breach of the Data Protection Act	Disciplined internally	No	No
		1	Officer	Complainant states that the police informed his employer of his arrest which caused the loss of his employment as a contract cleaner at a school.	Disciplined internally	No	No
		1	Officer	The officer has supplied a document to a third party which they were not entitled to have, albeit a legal representative for an officer who was subject to a criminal misconduct interview. Furthermore, he is a ********** and should be fully aware that this document is non disclosable and subject to legal privilege. He has no reason to access or obtain this document and indeed, it is clear on the MG3 that this is a report between the Police and the CPS and is Not Disclosable.	Disciplined internally	No	No
		1	Officer	Officer disclosed confidential information regarding a live misconduct matter	Disciplined internally	No	No

				involving another officer to a third party outside the MPS.			
		1	Officer	Asked another officer to access information, a request which contravened Data Protection Act and MetSec rules.	Disciplined internally	No	No
		1	Officer	The complainant states that an officer has breached the Data Protection Act and passed sensitive information to an external 3rd party.	Disciplined internally	No	No
		1	Officer	Complainant states that the officer sent confidential information to his medical school.	Disciplined internally	No	No
		1	Officer	Failure in duty - officer allowed another officer to use her log on and password to access a computer system to which a data protection act applies	Disciplined internally	No	No
		1	Civilian	Unsatisfactory performance - specifically breaches of the DPA.	Disciplined internally	No	No
		1	Civilian	Not following correct procedure and issuing a police officers private telephone number to a member of the public	Disciplined internally	No	No
		1	Civilian	Improper disclosure of information - Loser of motor vehicle has been	Disciplined internally	No	No

				given details of the finder by police, Breaching data protection and complainant's privacy.			
		1	Civilian	The complainant states that a member of police staff breached the data protection by disclosing the name and address of a witness to another witness relating to an offence of residential burglary.	Disciplined internally	No	No
		1	Civilian	Improper disclosure of information - Complainant's details were given to the other party concerned, and now (C) fears for her life	Disciplined internally	No	No
		1	Civilian	Claims officer turned his IT unit to the informant's sister and mother thereby disclosing the details of his caution. His family had been unaware of this matter until this time	Disciplined internally	No	No
		1	Civilian	Allegation of Breach of Data Protection and misuse of PNC.	Disciplined internally	No	No
		1	Civilian	The complainant states his address has been listed on a crime digest, in terms of road name, method and property taken, he is unhappy as he feels this breaches data protection and should not be in the	Disciplined internally	No	No

				public domain.			
		1	Civilian	(C) made a Data Protection Act application and has left messages but has not been updated by the officer	Disciplined internally	No	No
		1	Civilian	It is alleged that the subject breached the Data Protection Act.	Disciplined internally	No	No
		1	Civilian	The complainant states that the ********** gave her details to an alleged victim, this was in breach of the Date Protection Act.	Disciplined internally	No	No
		1	Civilian	Failed to call complaint back as promised and give incorrect advice around the notification of an adult in Police Custody contrary to the Data Protection Act.	Disciplined internally	No	No
		1	Officer	The complainant states that an officer breached Data Protection and/or Information sharing regulations.	Resigned during disciplinary	Yes	No
		1	Officer	Officer obtained information from the CRIS system to which he was not entitled with regard to the investigation of two rapes relating to a ********** and this information was	Resigned during disciplinary	Yes	No

				passed to an unknown person, both aspects being contrary to section 55 of Data Protection Act 1998.			
		1	Officer	Improper disclosure of information - It is alleged that PC ********* has made reference in media interviews to investigations that he may not have had any professional dealings with- this may have be in breach of data protection laws and principles.	Resigned during disciplinary	Yes	No
		1	Officer	Whilst completing a CRIS for theft of M/V at ********** station where the Victim was with other officers, ********** asked the male for his details. The victim provided ******** with his driving license. ******* returned to the office on the ********** where only himself and ********* were sat. ******* apparently found the males name amusing and was laughing and stated 'I NEED TO SEND THIS TO MY FRIEND' ********** has seen ********* take his phone, open to the 'SNAPCHAT' App and point	Resigned during disciplinary	Yes	No

				it towards the victims driving license to take a photo. ********** has challenged ********. ********* has advised ********** not to and ********** put his phone away. However ********** was in and out the office and did not have view of ********** at all times. This is a clear breach of data protection, it also falls far below the professional standards of the Metropolitan Police and is an abuse of trust.			
		1	Civilian	The subject accepted a Caution on ********* for breaching the Data Protection Act 1998.	Resigned during disciplinary	Yes	No
Norfolk Constabulary	**31**	1	Staff	Accessed personal data on force system for non-policing purpose	Dismissed	No	No
		1	Staff	Accessed force systems without policing purpose and disclosed the information	Dismissed	No	No
		2	Information not broken down	Accessed data systems without a lawful policing purpose	Disciplined internally[10]	No	No
		1		Accessed custody record without policing purpose and potentially disclosed the	Disciplined internally	No	No

[10] Response notes: 7 Police officers and 8 members of staff were disciplined internally.

				details to a third party			
		1		Browsing force systems regarding family/associates	Disciplined internally	No	No
		2		Accessed systems to view intelligence records for non-policing purpose	Disciplined internally	No	No
		2		Accessed systems for non-policing purpose	Disciplined internally	No	No
		2		Accessed systems to conduct intelligence searches for non-policing purpose	Disciplined internally	No	No
		1		Disclosure confidential information	Disciplined internally	No	No
		1		Accessed systems to conduct intelligence searches on individual and in relation to a specific incident	Disciplined internally	No	No
		1		Accessed systems to make intelligence checks for non-policing purpose	Disciplined internally	No	No
		1		Inappropriately accessed custody records relating to known individuals	Disciplined internally	No	No
		1		Utilised personal details for a non-policing purpose	Disciplined internally	No	No
		1		Accessed systems for non-policing purpose	Resigned during disciplinary process[11]	Yes	No
		1		Accessed data held on force system for a non-policing purpose	Resigned during disciplinary process	Yes	No
		1		Obtain/disclose personal data	Resigned during	Yes	No

[11] Response notes: 2 police officers and 2 members of staff resigned during the disciplinary process.

				from systems relating to intelligence checks	disciplinary process		
		1		Accessed systems to conduct intelligence searches for a non-policing purpose	Resigned during disciplinary process	Yes	No
		1		Accessed force systems for non-policing purpose and disclosed the data to a third party	No formal disciplinary action[12]	No	No
		1		Unlawful disclosure of sensitive personal data to another public authority	No formal disciplinary action	No	No
		2		Disclosed sensitive information	No formal disciplinary action	No	No
		1		Viewed police systems without policing purpose	No formal disciplinary action	No	No
		1		Inappropriate searches of force systems in respect of individuals and associated addresses	No formal disciplinary action	No	No
		1		Inappropriately accessed intelligence information relating to known individuals	No formal disciplinary action	No	No
		3		Accessed the custody system and viewed custody records for a non-policing purpose	No formal disciplinary action	No	No
North Wales Police	**25**	2	Police	Accessed police info for a non-policing purpose.	Final Written Warning	No	No
		2	Police	Accessed police info for a non-policing purpose.	Written warning and Management Action	No	No
		1	PCSO	Accessed and disclosed	Dismissed	No	No

[12] Response notes: 9 police officers and 1 member of staff received no formal disciplinary action.

				several pieces of police information to partner			
		1	Civilian	Accessed police info for a non-policing purposes. Had unsolicited communication with subjects of the access	Final Written Warning extension	No	No
		1	Police	Accessed police info for a non-policing purpose.	Written warning	No	No
		1	Civilian	Accessed police info for a non-policing purpose.	Final Written Warning	No	No
		1	Civilian	Accessed police info for a non-policing purpose.	Formal warning	No	No
		1	Civilian	Accessed police info for a non-policing purpose.	Verbal warning	No	No
		1	Police	Had information transcribed by external agency and disclosed personal data in the process	Management Advice	No	No
		1	Police	Accessed intel relating to criminal offences and disclosed to persons connected to the offences	Prosecuted and found guilty (Retired)	No	Yes
		1	Civilian	Accessed police info for a non-policing purpose	Verbal warning	No	No
		1	Police	Accessed police info and disclosed to partner	Officer was dismissed for other misconduct offence prior to this charge	No	No
		2	Civilian	Accessed police info for a non-policing purpose	Verbal warning	No	No
		1	Police	Accessed police info for a non-policing purpose	Meeting - Management Advice	No	No
		1	PCSO	Accessed police info for a non-	Verbal warning	No	No

				policing purpose			
		1	Police	Accessed police info for a non-policing purpose	Not proven - Management Action	No	No
		1	Civilian	Accessed police info for a non-policing purpose	Resigned before charges preferred	Yes	No
		1	Civilian	Accessed police info for a non-policing purpose	Dismissed	No	No
		1	Police	Accessed police info for a non-policing purpose	Dismissed	No	No
		1	Civilian	Accessed police info for a non-policing purpose	Resigned	Yes	No
		2	Police	Accessed police info for a non-policing purpose	Meeting - Management Advice	No	No
North Yorkshire Police	**98**	5	Refused - S. 40	Disclosed police information	Management Action	No	No
		1		Disclosed police information	Final Written Warning	No	No
		1		Disclosed police information	No Further Action	No	No
		21		Accessed police systems without a policing purpose	Management Action	No	No
		8		Accessed police systems without a policing purpose	Written Warning	No	No
		5		Accessed police systems without a policing purpose	Final Written Warning	No	No
		1		Accessed police systems without a policing purpose	Dismissal	No	No
		7		Accessed police systems without a policing purpose	No Further Action	No	No
		1		Loss of insecure memory stick	Written Warning	No	No
		12		Emailed Restricted/Confidential material to an insecure email address	Management Action	No	No
		1		Emailed	No Further Action	No	No

				Restricted/Confidential material to an insecure email address			
		1		Laptop Stolen	Management Action	No	No
		1		Unauthorised use of a Police System	Management Action	No	No
		1		Unauthorised use of a Police System	Written Warning	No	No
		1		Unauthorised use of a Police System	Dismissal	No	No
		14		Misuse of a Police System	Management Action	No	No
		8		Misuse of a Police System	Written Warning	No	No
		1		Misuse of a Police System	Final Written Warning	No	No
		2		Misuse of a Police System	Dismissal	No	No
		6		Misuse of a Police System	No Further Action	No	No
Northamptonshire Police	**24**	1	Staff	Police staff member misuse of force intelligence system.	Criminal Caution	No	Yes
		1	Staff	Improper access to force systems	Disciplined internally	No	No
		1	Officer	Misuse of Police system	Disciplined internally	No	No
		1	Staff	Improper disclosure of information	Disciplined internally	No	No
		2	Officer	Improper disclosure of information	Disciplined internally	No	No
		2	Officer	Improper disclosure of personal information	Disciplined internally	No	No
		1	Officer	Failure to disclose information	Disciplined internally	No	No
		1	Officer and Staff	Improper disclosure of personal information to a number of parties	Disciplined internally	No	No
		14	Information	Information not provided	No disciplinary action	No	No

			not provided				
Northumbria Police	**Refused - Cost and Time**						
Nottinghamshire Police[13]	**11**	1	Information not broken down	In receipt of 3rd party data about another individual. Inadvertent disclosure of incidents relating to another individual of the same name.	On review found to be a genuine mistake Action Memo to PSD re this incident and lessons learned.	No	No
		1		Inappropriate Disclosure of Information - Information sent to incorrect recipient. Sent request form re an investigation to the ICO instead of the LA, which outlined the crime.	Officer responsible should be given a formal guidance interview by line manager.	No	No
		1		Inappropriate Disclosure of Information - Disclosure of Third party information to another employee through accessing systems for unauthorised use.	Gross misconduct of staff member - Recipient of the information had a duty of care to report it and should be subject to disciplinary for failure to report the DPA breaches.	No	No
		1		Inappropriate Disclosure of Information - Inappropriate disclosure of information to the Universities in Nottingham	Closed and signed off by DCC	No	No
		1		Inappropriate use of Data - Inappropriate use of NHW scheme. Access information	Advice given. Genuine error	No	No

[13] Response notes: One further case is still under investigation.

				from Neighbour Hood watch scheme.			
		1		Loss / theft of Data - Possible theft of data from Police vehicle - Police information found to be missing from Vehicle	Signed off by DCC. Risk assessed. Advice given.	No	No
		1		Inappropriate use of Data - Notification from NCC in respect of whistle-blower report to ICO	This has been referred to the ICO	No	No
		1		Disclosure of information was made to Notts County Council instead of Notts City Council - however, both have entries for the 'child' and the County Council did confirm incorrectly they had made the request when contact by Police Disclosure Officer who was seeking confirmation.	Action send letter from SIRO to Notts County Courts Information Gov. Lead highlighting the need to specify full local authority detail of County Council or City Council to enable us to avoid inadvertent disclosure – Lessons learned discussion with Disclosure Team	No	No
		1		PC disclosed to third party that an individual had previous convictions	Officer resigned during the investigation.	Yes	No
		1		Inappropriate Disclosure of information - Correspondence from Professional Standards Department to incorrect address	PSD briefed all staff on ensuring that addresses are accurately recorded and kept up to date. There are now	No	No

					measures in place to send documents with personal and sensitive personal data by recorded or special delivery		
		1		Inappropriate disclosure of information – PC disclosed information in relation to individuals to third parties	Dismissed gross misconduct	No	No
Police Scotland[14]	**28**	1	Police	Misuse of police systems	Retired prior to completion of misconduct proceedings. Convicted.	No	Yes
		1	Police	Misuse of police systems	Resigned prior to completion of misconduct proceedings. Convicted.	Yes	Yes
		1	Police	Misuse of police systems	Police Conduct Regulation - Reduction in rate of pay. Convicted.	No	Yes
		1	Police	Misuse of police systems	Police Conduct Regulation Warning. Convicted.	No	Yes
		12	Police	Misuse of police systems	Police Conduct Regulation Warning	No	No
		1	Police	Misuse of police systems	Resigned prior to completion of	Yes	No

[14] Response notes: Question 5 refused due to cost and time limits.

					misconduct proceedings		
		1	Police	Misuse of police systems	Police Conduct Regulation - Fine	No	No
		4	Police	Misuse of police systems	Corrective advice	No	No
		1	Police Staff	Information not provided	Conviction	No	Yes
		1	Police Staff	Information not provided	Employment Terminated	No	No
		4	Police Staff	Information not provided	Disciplined internally	No	No
Police Service of Northern Ireland	**Refused - Cost and Time**						
South Wales Police	**67**	1	Police Staff	The subject inappropriately accessed relatives on system.	Written Warning	No	No
		1	Police Staff	The subject inappropriately accessed records of associates.	Subject Resigned during Investigation.	Yes	No
		1	Constable	The subject inappropriately accessed the record of an associate.	Written Warning	No	No
		1	Constable	The subject inappropriately accessed their former partner's details.	Written Warning	No	No
		1	Police Staff	The subject inappropriately accessed a system record pertaining to a relative.	Management Advice	No	No
		1	Constable	The subject inappropriately printed a copy of an incident pertaining to theirself.	Management Action	No	No
		1	Constable	The subject researched a family member without authorisation.	Management Advice	No	No
		1	Police Staff	The subject inappropriately	Subject Resigned	Yes	No

				accessed records of their partner.	during Investigation		
		1	Police Staff	The subject checked the database regarding an associate.	Subject Resigned during Investigation	Yes	No
		1	Constable	Personnel member requested information not for a Policing Purpose.	Management Action	No	No
		1	Constable	The subject inappropriately accessed the record of a personal matter not pertaining to their police duties.	Written Warning	No	No
		1	Police Staff	The subject inappropriately accessed the record of a family member.	Subject Resigned during Investigation	Yes	No
		1	Constable	The subject was alleged to be inappropriately accessing and disclosing police information to an associate.	Subject Resigned during Investigation.	Yes	No
		1	Sergeant	The subject inappropriately accessed a record pertaining to a relative.	Management Action	No	No
		1	Police Staff	The subject inappropriately accessed records pertaining to associates / premises.	Subject Resigned during Investigation.	Yes	No
		1	Constable	The subject made an inappropriate disclosure during a telephone conversation with a third party	Management Action	No	No
		1	Police Staff	The subject conducted unauthorised searches on an	Written Warning	No	No

				associate.			
		1	Constable	The subject inappropriately accessed the system records of family members.	Management Action	No	No
		1	Police Staff	The subject conducted an unauthorised search on an associate.	Written Warning	No	No
		1	Police Staff	Personnel member made unauthorised amendments to a record.	Subject Resigned during Investigation	Yes	No
		1	Constable	The subject inappropriately accessed records pertaining to their partner.	Written Warning	No	No
		1	Constable	The subject conducted unauthorised searches on family members.	Management Action	No	No
		1	Police Staff	The subject accessed a record pertaining to theirself.	Management Action	No	No
		1	Constable	The subject accessed the record of an associate for other than a policing purpose.	Written Warning	No	No
		1	Constable	The subject inappropriately accessed the record of a family member.	Management Action	No	No
		1	Constable	The subject accessed and disclosed restricted information.	Dismissal Without Notice. Criminal caution given	No	No
		1	Constable	The subject conducted checks on associates for other than a policing purpose.	Management Action	No	No
		1	Staff	The subject checked a third party on a database not for a Policing Purpose	Management Action	No	No

		1	Police Staff	The subject made improper comments to an associate.	Subject Dismissed from SWP	No	No
		1	Constable	The subject accessed a record without authorisation to do so.	Management Action	No	No
		1	Police Staff	The subject made unauthorised checks on associates for a non-Policing purpose.	Subject Dismissed from SWP	No	No
		1	Constable	The subject made unauthorised access to records.	Management Advice	No	No
		1	Police Staff	The subject accessed the record of an associate without authorisation.	Subject Resigned during Investigation	Yes	No
		1	Police Staff	The subject accessed records of incidents without authorisation to do so.	Final Written Warning	No	No
		1	Police Staff	The subject accessed records of their former partner without authorisation.	Management Action	No	No
		1	Police Staff	The subject accessed the record of a family member without authorisation.	Final Written Warning	No	No
		1	Constable	The subject inappropriately made access to their partner's record without authorisation.	Management Action	No	No
		1	Constable	Officer accessed records for a non-policing purpose / in breach of force policy.	Resigned during Investigation, processed and convicted criminally.	Yes	Yes
		1	Constable	Officer accessed records for a non-policing purpose / in	(Allegation a component of a multi-	No	No

				breach of force policy.	tier case) Dismissal without Notice		
		1	Constable	Officer accessed records for a non-policing purpose / in breach of force policy.	Final Written Warning	No	No
		1	Staff	Made comments in public regarding an individual's criminal status that were not appropriate for disclosure.	Management Action	No	No
		1	Staff	Made comments in public regarding their duties that were a breach of confidentiality.	Management Action	No	No
		1	Police Staff	Staff member accessed information for reasons other than Policing Purpose	First Written Warning	No	No
		1	Police Officer	Did not secure sensitive interview discs relating to an inquiry, leading to their loss.	Management Action	No	No
		1	Police Staff	Accessed the data record of a colleague without a Policing Purpose.	Final Written Warning	No	No
		1	Constable	Accessed records relating to a relative without a Policing purpose.	Resigned during Investigation	Yes	No
		1	Police Staff	Accessed record relating to a family member without a Policing Purpose.	Management Action	No	No
		1	Police Staff	Accessed the record of a relative without a Policing purpose.	Written Warning	No	No
		1	Police Staff	Resigned during Investigation	Resigned during Investigation	Yes	No

		1	Police Staff	Inadvertently verbally disclosed information relating to a MOP's private life during an inquiry.	Management Action	No	No
		1	Police Staff	Accessed the record of her partner without a policing purpose.	Written Warning	No	No
		1	Police Staff	Accessed the records of family members without a Policing Purpose, and spoke indiscreetly and without due caution to Data Protection when in public.	Written Warning	No	No
		1	Constable	Accessed the record of his partner and home location without a Policing Purpose.	Management Action	No	No
		1	Constable	The subject accessed the records of the partner of a relative without a Policing purpose, this was linked to an ongoing welfare concern and the subject believed it was within the Purpose criteria. Management Action given.	Management Action	No	No
		1	Constable	Subject looked at the record of an associate without a Policing purpose.	Management Action	No	No
		1	Police Staff	Browsed' records on a police system without a Policing Purpose.	Written Warning	No	No
		1	Constable	Made multiple disclosures of protected information to a relative, he received criminal	Dismissal without Notice. Criminal caution given.	No	No

				caution.			
		1	Constable	Disclosed Police information to her partner.	Management Action	No	No
		1	Police Staff	Photographed and disseminated restricted documentation for personal gain.	Dismissal without Notice	No	No
		1	Constable	Accessed records of relatives without a Policing Purpose.	Management Action	No	No
		1	Special Constable	Made a comment on a social networking site which could potentially have breached confidentiality.	Management Action	No	No
		1	Constable	Property was returned to the relative of a detainee that contained personal information.	Management Action	No	No
		1	Constable	Accessed the record of his partner without a Policing Purpose to do so.	Written Warning	No	No
		1	Constable	Disclosed the results of a medical report to Next of Kin without the FLO's consent.	Management Action	No	No
		1	Constable	Accessed information relating to former partner without a Policing Purpose.	Management Action	No	No
		1	Police Staff	Sent an email to colleagues without first removing a sensitive attached document from the email chain.	Management Action	No	No
		1	Police Staff	Checked partner on a police database without a policing purpose.	Written Warning	No	No

South Yorkshire Police	**50**	1	Officer	Accessed information not in the course of his/her duties.	Guilty plea - fine, surcharge & costs	No	Yes
		1	Staff	Accessed policing system for non-policing purpose and disclosed personal information	Caution	No	No
		1	Staff	It was alleged that the member of staff might have passed information to a third party.	Attended Misconduct Hearing and dismissed	No	No
		1	Staff	Conducted a police check for a non-policing purpose.	Written Warning	No	No
		1	Staff	Accessed police systems for non-policing purposes.	Written Warning	No	No
		1	Officer	Conducted police checks for a non-policing purpose	Final Written Warning	No	No
		1	Officer	Accessed systems for non-policing purposes.	Written Warning	No	No
		1	Staff	Carried out checks on policing system for no policing purposes	Written Warning	No	No
		2	Officer	Accessed police system for non-policing purpose	Final Written Warning	No	No
		1	Officer	Allegation that an Officer has accessed policing systems and disclosed Complainant's confidential information to another	Final Written Warning	No	No
		1	Officer	Allegation that an Officer has accessed policing systems and inappropriately disclosed Complainant's data to a third party.	Final Written Warning	No	No

		1	Officer	Allegation that an Officer used a police system to obtain personal information about Complainant for a non-policing purpose	Final Written warning	No	No
		1	Officer	The officer is believed to have disclosed information relating to policing tactics and utilised police systems for a non-policing purpose when conducting checks.	Resigned during disciplinary procedures	Yes	No
		2	Officer	The officer accessed information for a non-policing purpose	Resigned during disciplinary procedures	Yes	No
		1	Staff	The member of staff accessed Complainant's information on police system, for a non-policing purpose.	Resigned during disciplinary procedures	Yes	No
		1	Staff	Released an incorrect 'suspect' image via Media	Management Advice	No	No
		1	Officer	Used policing systems for a non-policing purpose.	Management Advice	No	No
		2	Officer	The Officer did not have a legitimate policing purpose for conducting a vehicle check	Negative Personal Development Journal	No	No
		1	Officer	The Officer used police systems for non-policing purposes.	Management advice	No	No
		1	Officer	The Officer accessed police system for a non-policing purpose.	No action	No	No
		1	Officer	It is alleged that the Officer used a policing system for a	Management advice	No	No

				no policing purpose			
		1	Officer	It is alleged that whilst off duty, an Officer has used mobile device to conduct a check on a vehicle.	Advice given	No	No
		1	Officer	Allegation that an Officer has used police systems for no policing purpose.	Negative Personal Development Journal	No	No
		1	Officer	Officer failed to maintain proper control of hardcopy paperwork extracted from a policing system. The failure allowed personal data to be accessed by third party.	Negative Personal Development Journal	No	No
		1	Staff	Accessed police systems for a non-policing purpose	No action	No	No
		1	Officer	Accessed police systems for a non-policing purpose	Negative Personal Development journal	No	No
		1	Special Constable	Accessed police systems for a non-policing purpose	No action	No	No
		1	Officer	Accessed police systems with no legitimate reason for doing so	Advice given	No	No
		1	Staff	It is alleged that the member of Staff accessed police systems for a non-policing purpose	No Action	No	No
		1	Staff	It is alleged that the member of Staff used police systems for a non-policing purpose.	Advice given	No	No
		1	Officer	It is alleged that the Officer passed confidential information obtained from	No action	No	No

				police systems to a third party.			
		1	Officer	The Officer is alleged to have communicated information gained due to his/her role, outside of the organisation	Advice given	No	No
		1	Officer	It is alleged that the Officer used police systems for a no policing purpose	Advice given	No	No
		1	Staff	An allegation that a member of Staff has disclosed the Complainant's information, which is inaccurate, to the media	No action	No	No
		1	Officer	The complainant alleges that the police have passed his/her address to a third party	No action	No	No
		1	Officer	An allegation that the Officer disclosed personal information about the Complainant to his/her neighbour.	No action	No	No
		1	Officer	An allegation that the Officer has divulged the Complainant's personal information to a third party.	No Action	No	No
		1	Officer	An allegation that the Officer improperly disclosed information regarding the Complainant, whilst in public place	No Action	No	No
		1	Officer	An allegation that the Officer disclosed confidential	No action	No	No

				information about a family member to third parties.			
		1	Officer	An allegation that the Officer has passed the Complainant's address/phone number to a third party.	No Action	No	No
		1	Staff	An allegation that personal data was inappropriately disclosed to the Complainant's employer.	No Action	No	No
		1	Officer	An allegation that the Officer disclosed personal data for no legitimate purpose.	No Action	No	No
		1	Officer	An allegation that the Officer inappropriately passed Complainant's information on to a third party	No Action	No	No
		1	Officer	An allegation that the Officer has passed the Complainant's personal information about him to third parties.	No Action	No	No
		2	Officer	An allegation that Officers inappropriately discussed/disclosed the Complainant's personal information to a third party.	No Action	No	No
		1	Officer	An allegation that the Officer inappropriately disclosed information regarding individuals within the Complainant's vicinity	No Action	No	No
Staffordshire Police	**31**	4	Police officer	Accessed internal systems for non-police purpose	Disciplined internally	No	No

		1	Police officer	Allowed another person access to sensitive documents/photographs	Disciplined internally	No	No
		1	Police officer	Accessed internal record of former colleague	Disciplined internally	No	No
		1	Police officer	Information from police system passed to another person	Disciplined internally	No	No
		2	Police officer	Accessed internal systems for non-police purpose	Resigned during disciplinary procedure	Yes	No
		1	Police staff	Inadvertently allowed another person view of confidential paperwork	Management advice given	No	No
		1	Police staff	Accessed information relating to an individual	Resigned during disciplinary procedure	Yes	No
		1	Police officer	Used position to obtain and provide information to another person	Disciplined internally	No	No
		1	Police officer	Accessed information and disclosed to another person	Disciplined internally	No	No
		1	Police officer	Accessed police information without lawful purpose	Convicted for breaches of Data Protection Act 1998. Employment terminated.	No	No
		1	Police officer	Inappropriate use of police systems	Disciplined internally	No	No
		1	Police officer	Accessed internal system and viewed records without police purpose	Disciplined internally	No	No
		1	Police officer	Accessed internal system to gather information without police purpose	Disciplined internally	No	No

		1	Police officer	Attempt to coerce other staff members to access internal information for non-police purpose	Disciplined internally	No	No
		1	Police officer	Disclosed information to another person	Disciplined internally	No	No
		1	Police staff	Accessed internal records for personal interest	Disciplined internally	No	No
		1	Police officer	Permitted another individual to access police systems	Disciplined internally	No	No
		1	Police staff	Accessed information and may have disclosed to another person	Resigned during disciplinary procedure	Yes	No
		1	Police staff	Unauthorised disclosure to third party	Information not provided	No	No
		1	Police staff	Access IT systems for non-police purpose	Disciplined internally	No	No
		1	Police officer	Disclosed confidential/tactical information to another person	Disciplined internally	No	No
		1	Police staff	Access internal systems for non-police purpose	Resigned during disciplinary procedure	Yes	No
		1	Police staff	Viewed internal systems for non-policing purpose	Disciplined internally	No	No
		1	Police officer	Disclosed confidential information to another person	Convicted for breaches of Data Protection Act 1998. Employment terminated.	No	No
		1	Police officer	Lost bodycam	Management advice given	No	No
		1	Police staff	Inadvertently emailed attachment to third party	Management advice given	No	No
		1	Police staff	Inadvertently provided	Management advice	No	No

				confidential information to a third party	given		
Suffolk Constabulary	**27**	1	Information not broken down	Accessed systems without a legitimate policing purpose	Convicted[15]	No	Yes
		1		Obtaining/disclosing personal data	Convicted	No	Yes
		1		Accessed systems for a non-policing purpose	Convicted	No	Yes
		2		Accessed force systems for a non-policing purpose	Dismissed[16]	No	No
		1		Accessed and disclosed information gained from force systems for non-policing purpose	Dismissed	No	No
		1		Unlawfully accessed force systems viewing data	Disciplined internally[17]	No	No
		1		Accessed force systems for non-policing purpose.	Disciplined internally	No	No
		1		Sent internal email to a colleague with reference to an arrest which has no policing purpose.	Disciplined internally	No	No
		2		Accessed force systems to conduct intelligence searches for a non-policing purpose	Disciplined internally	No	No
		1		Accessed force systems to search criminal records for a non-policing purpose	Disciplined internally	No	No
		1		Accessed force systems to	Disciplined internally	No	No

[15] Response notes: 2 police officers and 1 member of staff were convicted.
[16] Response notes: 1 police officer and 2 members of staff were dismissed.
[17] Response notes: 4 police officers and 4 members of staff were disciplined internally.

				obtain data for a non-policing purpose.			
		1		Accessed force systems to obtain confidential data	Disciplined internally	No	No
		1		Accessed crimes and other force systems for non-policing purpose and relayed information to a named nominal	Resigned during disciplinary[18]	Yes	No
		1		Accessed force system records for non-policing purpose	Resigned during disciplinary	Yes	No
		1		Disclosed sensitive data to members of the of the public and researched systems for non-policing purpose	Resigned during disciplinary	Yes	No
		1		Improper disclosure of information	Resigned during disciplinary	Yes	No
		2		Accessed police records for non-policing purpose	Resigned during disciplinary	Yes	No
		1		Accessed force systems for non-policing purpose	Resigned during disciplinary	Yes	No
		1		Accessed force systems to conduct intelligence searches for non-policing purpose	Resigned during disciplinary	Yes	No
		1		Accessed and disclosed information obtained from force systems without policing purpose	Resigned during disciplinary	Yes	No
		1	Police	Disclosed personal information to complainant's employer	No disciplinary action	No	No

[18] Response notes: 5 police officers and 3 members of staff resigned during disciplinary proceedings.

		1	Police	Accessed force intelligence systems for non-policing purpose	No disciplinary action	No	No
		1	Police	Accessed force systems for non-policing purpose	No disciplinary action	No	No
		1	Police	Made disclosure of information to a third person	No disciplinary action	No	No
		1	Police	Improper disclosure of information	No disciplinary action	No	No
		1	Police	Accessed force systems for non-policing purpose	No disciplinary action	No	No
Surrey Police	**202**	2	Civilian	Accessing police systems without a policing purpose. Personal details and linked police reports.	Live investigation	N/A	N/A
		2	Police	Inappropriately sharing information with a third party. Operational deployments, availability of equipment and training details.	Live investigation	N/A	N/A
		5	Civilian	Accessing police systems without a policing purpose. Personal details and linked police reports.	First Written Warning	No	No
		2	Civilian	Accessing police systems without a policing purpose. Personal details and linked police reports.	Not proven	No	No
		1	Civilian	Accessing police systems without a policing purpose. Vehicle and user information.	Final Written Warning	No	No
		21	Police	Accessing police systems without a policing purpose.	Management Advice	No	No

				Personal details and linked police reports.			
		12	Police	Accessing police systems without a policing purpose. Personal details and linked police reports.	Written Warning	No	No
		1	Civilian	Accessing police systems without a policing purpose. Personal details and linked police reports.	No action	No	No
		3	Police	Accessing police systems without a policing purpose. Crime report.	No action	No	No
		1	Police	Accessing police systems without a policing purpose. Crime report.	Management Action	No	No
		6	Police	Accessing police systems without a policing purpose. Personal details and linked police reports.	Final Written Warning	No	No
		1	Police	Inappropriately sharing information relating to operational policing. Name, location and description of police business.	Dismissed	No	No
		17	Police	Accessing police systems without a policing purpose. Personal details and linked police reports.	Dismissed	No	No
		4	Police	Accessing police systems without a policing purpose. Crime report.	Management Advice	No	No
		1	Police	Accessing police systems	Dismissed	No	No

				without a policing purpose. Crime report.			
		4	Police	Accessing police systems without a policing purpose. Personal details and linked police reports.	No action	No	No
		1	Police	Accessing police systems without a policing purpose. Crime report.	Not proven	No	No
		12	Police	Accessing police systems without a policing purpose. Crime report.	Management Intervention	No	No
		10	Civilian	Accessing systems without a policing purpose. Personal details and linked police reports.	Dismissed	No	No
		5	Police	Accessing police systems without a policing purpose. Crime report.	Written Warning	No	No
		7	Civilian	Accessing police systems without a policing purpose. Personal details and linked police reports.	Resigned	Yes	No
		1	Civilian	Accessing police systems without a policing purpose. Crime report.	Resigned	Yes	No
		1	Civilian	Using police systems under another person's details. Personal details and linked police reports.	Resigned	Yes	No
		4	Civilian	Accessing police systems without a policing purpose. Personal details and linked	Final Written Warning Extension	No	No

				police reports.			
		2	Police	Accessing systems without a policing purpose. Personal details and linked police reports.	First Written Warning	No	No
		30	Police	Accessing police systems without a policing purpose. Personal details and linked police reports.	Management Intervention	No	No
		2	Police	Accessing systems without a policing purpose. Personal details and linked police reports.	Retired	No	No
		1	Civilian	Accessing systems without a policing purpose. Personal details and linked police reports.	Formal Verbal Warning	No	No
		1	Civilian	Inappropriately sharing information with a third party. Identity of detained person.	Written Warning	No	No
		1	Civilian	Inappropriately sharing information with a third party. Information of an alleged previous conviction	Final Written Warning	No	No
		1	Civilian	Accessing systems without a policing purpose. Personal details and linked police reports.	Final Written Warning	No	No
		3	Police	Accessing systems without a policing purpose. Records of crime and nominals in the area	Management Intervention	No	No
		8	Civilian	Accessing systems without a	No action	No	No

				policing purpose. Personal details and linked police reports.			
		1	Civilian	Accessing systems without a policing purpose. Personal details and linked police reports.	Management Action	No	No
		1	Civilian	Accessing police systems without a policing purpose. Crime report.	Management Action	No	No
		1	Police	Accessing police systems without a policing purpose. Crime report.	Management Action	No	No
		1	Civilian	Accessing police systems without a policing purpose. Personal details and call logs	Management Action	No	No
		1	Civilian	Inappropriately sharing information with a third party. Vehicle owner and insurance details.	Management Action	No	No
		1	Police	Accessing systems without a policing purpose. Personal details and linked police reports.	Management Action	No	No
		13	Civilian	Accessing systems without a policing purpose. Personal details and linked police reports.	Management Intervention	No	No
		4	Civilian	Accessing systems without a policing purpose. Crime report.	Management Intervention	No	No
		1	Civilian	Accessing police systems without a policing purpose.	Management Intervention	No	No

				Vehicle owner and insurance details			
		1	Police	Sending information to an insecure email address. Probationer documents.	Management Intervention	No	No
		1	Civilian	Disclosure of information in court. Financial information.	Unknown - Training package created handling of information.	No	No
		1	Police	Operational information left at the home address of a member of the public. Operational information.	Information not provided	No	No
		1	Police	Operational information left at the home address of a member of the public. Information relating to an investigation.	Management Action	No	No
		1	Civilian	Information accidentally shared with a third party via email. Confidential information.	Words of Advice	No	No
Sussex Police	**63**	6	Civilian	Information cannot be provided	Dismissed	No	No
		10	Civilian	Information cannot be provided	Disciplinary sanction	No	No
		8	Civilian	Information cannot be provided	Resigned	Yes	No
		15	Civilian	Information cannot be provided	No disciplinary action	No	No
		4	Civilian	Information cannot be provided	Case ongoing	N/A	N/A

		1	Police	Officer has made unlawful access to IT systems for personal reasons	Officer pleaded guilty at court and was fined. Officer resigned from Sussex Police	Yes	Yes
		1	Police	Officer inappropriately accessed police computer systems in order to response to a query from a friend involved in the matter	Officer dismissed without notice following misconduct hearing	No	No
		1	Police	Officer made inappropriate access to personal records contained within the crime and intelligence management system without a genuine policing purpose	Officer appeared before a misconduct hearing - Not proved - no further action	No	No
		1	Police	Officer made unlawful access to a report. It is believed this was for personal reasons.	Officer attended a misconduct meeting - Proven - received a written warning	No	No
		1	Police	Officer conducted a check on the Police National Computer on his personal vehicle, that was assessed as not for lawful policing purposes, but for personal reasons	Officer attended a misconduct meeting - Proven - received management advice	No	No
		1	Police	Officer undertook a number of enquiries on police computer systems without appropriate purpose or authority and disclosed personal information related to the suspect.	Officer attended a misconduct meeting - Proven - received a written warning	No	No

		1	Police	Officer inappropriately accessed IT systems in relation to a crime where the officer was recorded as he victim. The access was unlawful and for personal reasons.	Officer attended a misconduct meeting - Proven - received a written warning	No	No
		1	Police	Officer has, on multiple occasions, accessed police data relation to a neighbour dispute without legitimate purpose.	Officer attended a misconduct meeting - Proven - received a written warning	No	No
		1	Police	Officer accessed a number of documents on an IT system linked to the victim. This was not for a policing purpose.	Officer attended a misconduct meeting - Proven - received a final written warning	No	No
		1	Police	Officer accessed police IT systems, namely to search details of 4 people and an address, without lawful policing purpose.	Officer attended a misconduct meeting - Proven - received a written warning	No	No
		1	Police	Officer accessed computer records, following a separate investigation, for the subject of that investigation at a later date without legitimate policing purpose	Officer attended a misconduct meeting - Proven - received management advice	No	No
		1	Police	Officer made a series of entries to a computer system in order to identify a record relating to a relative and then re-accessed a report of an investigation of assault, again relating to the relative. This	Officer attended a misconduct meeting - Proven - received a written warning	No	No

				access was made for non-policing purpose and without lawful authority.			
		1	Police	Officer accessed IT systems for personal reasons regarding a reported theft where the officer was the victim.	Officer attended a misconduct meeting - Proven - received a final written warning	No	No
		1	Police	Officer accessed nominal records relating to a member of public without a lawful purpose.	Officer attended a misconduct meeting - Proven - received a final written warning	No	No
		1	Police	Officer has, on multiple occasions, accessed police systems in relation to a personal friend and ex-partner without legitimate policing purpose.	Officer attended a misconduct meeting - Proven - no further action	No	No
		1	Police	Officer accessed personal data on a police IT system for a non-authorised purpose. Officer also, on multiple occasions, accessed police data regarding incidents at their home address via a search.	Officer attended a misconduct meeting - Proven on both counts - received management advice and a written warning	No	No
		1	Police	Officer accessed police databases to obtain personal information relating to a complainant	Officer attended a misconduct meeting - Proven - received a written warning	No	No
		1	Police	Officer conducted a check on the Police National Computer in the absence of a lawful	Officer attended a misconduct meeting - Proven - received a	No	No

				policing purpose.	written warning		
		1	Police	Officer unlawfully accessed databases and further accessed the address record of a member of public.	Officer attended a misconduct meeting - Proven - received a final written warning	No	No
		1	Police	Officer inappropriately accessed computer systems to obtain address details of a complainant and disclosed the information to a family member.	Officer attended a misconduct meeting - Proven - received management advice	No	No
Thames Valley Police	**Refused - Cost and Time**						
Warwickshire Police	**17**	1	Police Officer	Alleges inappropriate disclosure of personal information to third party	Management advice given	No	No
		1	Civilian	Disclosure of confidential information via email to a computer not on a secure network	Final Written Warning	No	No
		1	Civilian	Reviewed information on force systems not for policing purpose	Verbal Warning	No	No
		1	Police Office	Unauthorised Police National Computer checks	Dismissed and convicted	No	Yes
		1	Civilian	Alleged divulgence of personal information where others could hear	First Written Warning	No	No
		1	Civilian	Inappropriate disclosure of information.	Informal Action	No	No
		1	Officer	Alleged divulgence of personal	Local Resolution - by	No	No

				information where others could hear	Division		
		1	Officer	Alleged divulgence of personal information where others could hear	Local Resolution - by Division	No	No
		1	Officer	Alleged divulgence of personal information to third party	Dispensation - by Force	No	No
		2	Officer	Alleged divulgence of personal information to third party	Local Resolution - by Division	No	No
		4	Officer	Alleged divulgence of personal information to third party	Management Action	No	No
		1	Civilian	Alleged divulgence of personal information to third party	Management Action	No	No
		1	Officer	Reviewed information on force systems not for policing purpose	Management Action - Misconduct	No	No
West Mercia Constabulary	**73**	1	Police	Misusing police systems in order to supply a member of the public	Management Advice	No	No
		1	Police	Personal checks on police systems	Dismissed	No	No
		1	Police	Breach of data protection	Final Written Warning	No	No
		2	Civilian	Accessed force systems to check and individual. Not done for a policing purpose	Verbal Warning	No	No
		1	Police	Accessed force systems to check and individual. Not done for a policing purpose	Dismissed	No	No
		1	Police	Requests for a PNC check, not for a policing purpose.	Written Warning	No	No
		1	Civilian	Police data access was for a non-policing purpose.	Final Written Warning	No	No

		1	Police	Accessed information from GENIE and passed it on	Management Advice	No	No
		1	Police	Accessing logs and records for a non-policing purpose	Management Advice	No	No
		1	Civilian	Accessing logs and records for a non-policing purpose	Final Written Warning	No	No
		1	Police	Accessed force systems to check an individual/s. Not done for a policing purpose.	Management Advice	No	No
		1	Civilian	Not all OIS use had been conducted for a policing purpose	Final Written Warning	No	No
		1	Civilian	Issues relating misuse of computer systems.	First Written Warning	No	No
		1	Police	OIS logs have been accessed by the officer for non-policing purposes.	Final Written Warning	No	No
		1	Civilian	Accessing logs for a non-policing purpose	Final Written Warning	No	No
		1	Police	Accessed force systems to check an individual. Not done for a policing purpose.	Management Advice	No	No
		1	Police	West Mercia Police documents recovered from an address	Written Warning	No	No
		1	Police	Accessed force systems to check an individual. Not done for a policing purpose.	Written Warning	No	No
		1	Police	Breached Data Protection act and passed information to outside individual.	Written Warning	No	No
		1	Civilian	Accessed GENIE data on known nominals which may	Final Written Warning	No	No

				have been for a non-policing purpose			
		1	Police	Checks on Genie not for a policing purpose	Dismissed	No	No
		1	Civilian	System audits suggest that individual has accessed police information for non-policing purposes	Verbal Warning	No	No
		1	Civilian	Accessed force systems. Not done for a policing purpose.	First Written Warning	No	No
		1	Civilian	19 separate Data Protection Act offences for a period	Dismissed and cautioned	No	No
		1	Police	Accessed force systems. Not done for a policing purpose.	Written Warning	No	No
		1	Police	Use of QAS for a non-policing purpose	Dismissal Without Notice	No	No
		1	Police	Genie check on officer's niece.	Final Written Warning	No	No
		1	Police	Accessed force systems to check an individual. Not done for a policing purpose.	Management Advice	No	No
		1	Civilian	There is information to suggest that a member of Police Staff has tried to obtain details from Police systems through a colleague that was not for a policing purpose.	First Written Warning	No	No
		1	Police	Evidence suggests the officer may have accessed force systems without a policing purpose.	Final Written Warning	No	No
		2	Civilian	Accessing logs for a non-policing purpose	Retired/Resigned	Yes	No

		1	Civilian	Incorrect copying and distributing of CCTV footage	Retired/Resigned	Yes	No
		1	Police	Accessed force systems to check an individual/s. Not done for a policing purpose	Retired/Resigned	Yes	No
		1	Police	Personal information has been passed to third parties	Local Resolution - by Division	No	No
		1	Civilian	Breach of Confidentiality and Data Protection	Local Resolution - by Division	No	No
		1	Police	A disclosure made within the sight and hearing of complainants family member	Local Resolution - by Division	No	No
		4	Police	Inappropriate disclosure of information	Local Resolution - by Division	No	No
		1	Police	Information has been inappropriately collated and disclosed.	Management Action - Misconduct	No	No
		1	Police	WMP sent out another's convictions and fines.	Local Resolution - by Division	No	No
		1	Police	Officer has breached confidentiality by disclosing address inappropriately	Local Resolution - by Division	No	No
		3	Police	breach of data protection	Local Resolution - by Division	No	No
		2	Police	Accessed force systems to check an individual/s. Not done for a policing purpose.	Local Resolution - by Division	No	No
		3	Police	Complaint police officers have disclosed to others they have reported a person for offence/s	Local Resolution - by Division	No	No
		1	Civilian	Information was disclosed, that complainant felt to be	Local Resolution - by Division	No	No

				inappropriate and unnecessary.			
		1	Civilian	Inappropriate disclosure of information	Management Action/Informal Action	No	No
		1	Police	Data may have been compromised through being filmed and transmitted.	Local Resolution - by Division	No	No
		1	Police	Genie record accessed for a non-policing purpose	Management Action	No	No
		2	Police	Accessed genie data on themselves. Not for a policing purpose.	Management Action	No	No
		1	Civilian	Accessed force systems to check an individual/s. Not done for a policing purpose.	Management Action/Informal Action/ UPP	No	No
		1	Civilian	Inappropriate circulation of personal information.	Management Action/Informal Action	No	No
		1	Police	Inappropriate circulation of police information	Management Action	No	No
		1	Civilian	Access of employee/s personal information for non-policing purpose	Management Action/ Informal Action	No	No
		1	Civilian	Disclosure of information to a third party that may have come from force systems.	Management Action/ Informal Action	No	No
		1	Police	Accessed a Genie record with no policing purpose. Data protection offence.	Management Action	No	No
		1	Police	Inappropriate possession of investigation material	Management Action	No	No
		3	Police	Accessed force systems to check an individual/s. Not done for a policing purpose.	No action	No	No

		1	Civilian	Inappropriate disclosure of address	Management Action/ Informal Action	No	No
		2	Civilian	Accessed force systems to check an individual/s. Not done for a policing purpose.	Management Action/ Informal Action	No	No
		1	Police	Inappropriate disclosure of investigation details	Management Action/ UPP	No	No
		1	Police	Accessed force systems to check an individual/s. Not done for a policing purpose.	Management Action	No	No
West Midlands Police	**488**	8	Police	07 Confidentiality	Formal Action. Dismissal Without Notice.	No	
		3	Police	07 Confidentiality	Formal Action. Dismissal Without Notice. Criminal Conviction.	No	Yes
		7	Police	07 Confidentiality	Formal Action. Final Written Warning.	No	No
		4	Police	07 Confidentiality	Formal Action. Management Advice.	No	No
		7	Police	07 Confidentiality	Formal Action. Written Warning.	No	No
		49	Police	07 Confidentiality	Management Action	No	No
		38	Police	07 Confidentiality	No Action	No	No
		2	Police	07 Confidentiality	Retired/Resigned	Yes	No
		1	CIV	07 Confidentiality	Dismissal Without Notice. Criminal Conviction.	No	Yes
		1	CIV	07 Confidentiality	Formal Action. Compulsory redundancy.	No	No

	2	CIV	07 Confidentiality	Formal Action. Dismissal Without Notice.	No	No
	1	CIV	07 Confidentiality	Formal Action. Dismissal Without Notice. Criminal Conviction.	No	Yes
	1	CIV	07 Confidentiality	Formal Action. Final Written Warning Extension.	No	No
	2	CIV	07 Confidentiality	Formal Action. Final Written Warning.	No	No
	3	CIV	07 Confidentiality	Formal Action. No Action	No	No
	2	CIV	07 Confidentiality	Formal Action. Required to resign.	Yes	No
	2	CIV	07 Confidentiality	Formal Action. Written Warning.	No	No
	12	CIV	07 Confidentiality	Management Action	No	No
	17	CIV	07 Confidentiality	No Action	No	No
	1	CIV	07 Confidentiality	No Action. Resigned. Criminal Conviction.	Yes	Yes
	1	CIV	07 Confidentiality	Retired/Resigned	Yes	No
	1	PCSO	07 Confidentiality	Formal Action. Dismissal Without Notice. Criminal Conviction.	No	Yes
	2	PCSO	07 Confidentiality	Management Action	No	No
	1	PCSO	07 Confidentiality	Management Action. Management Advice.	No	No
	2	PCSO	07 Confidentiality	No Action	No	No
	5	Police	Improper disclosure of	Case to Answer.	No	No

			information	Formal Action		
	9	Police	Improper disclosure of information	Case to Answer. Management Action.	No	No
	4	Police	Improper disclosure of information	Dispensation - by IPCC. No Action	No	No
	2	Police	Improper disclosure of information	Discontinued - by Force. No Action.	No	No
	2	Police	Improper disclosure of information	Disapplication - by Force. No Action.	No	No
	2	Police	Improper disclosure of information	Formal Action. Case to Answer.	No	No
	23	Police	Improper disclosure of information	Local Resolution - by Division. No Action.	No	No
	7	Police	Improper disclosure of information	Local Resolution - by PSD. No Action	No	No
	6	Police	Improper disclosure of information	Management Action. Case to Answer.	No	No
	1	Police	Improper disclosure of information	Management Action. Local Resolution - by Division.	No	No
	1	Police	Improper disclosure of information	Management Action. No Case to Answer.	No	No
	7	Police	Improper disclosure of information	No Action. Disapplication - by Force.	No	No
	4	Police	Improper disclosure of information	No Action. Local Resolution - by Division.	No	No
	2	Police	Improper disclosure of information	No Action. Local Resolution - by PSD.	No	No
	54	Police	Improper disclosure of information	No Action. No Case to Answer.	No	No

	4	Police	Improper disclosure of information	No Action. Withdrawn - by Force.	No	No
	8	Police	Improper disclosure of information	No Case to Answer. Management Action.	No	No
	116	Police	Improper disclosure of information	No Case to Answer. No Action.	No	No
	2	Police	Improper disclosure of information	Substantiated. Management Action.	No	No
	2	Police	Improper disclosure of information	Unsubstantiated. No Action.	No	No
	8	Police	Improper disclosure of information	Withdrawn - by Force. No Action.	No	No
	3	Police	Improper disclosure of information	Withdrawn - Not proceeded with. No Action.	No	No
	6	Police	Improper disclosure of information	Withdrawn. No Action.	No	No
	1	N/S	Improper disclosure of information	No Case to Answer. No Action.	No	No
	3	N/S	Improper disclosure of information	Unsubstantiated. No Action.	No	No
	1	CIV	Improper disclosure of information	Case to Answer. No Action.	No	No
	1	CIV	Improper disclosure of information	Case to Answer. Retired/Resigned.	Yes	No
	1	CIV	Improper disclosure of information	Disapplication - by Force. No Action.	No	No
	1	CIV	Improper disclosure of information	Management Action. Case to Answer.	No	No
	5	CIV	Improper disclosure of information	No Action. No Case to Answer.	No	No
	2	CIV	Improper disclosure of	No Action. Withdrawn	No	No

				information	- by Force.		
		3	CIV	Improper disclosure of information	No Case to Answer. Management Action.	No	No
		11	CIV	Improper disclosure of information	No Case to Answer. No Action.	No	No
		1	PCSO	Improper disclosure of information	Local Resolution - by Division. Management Action.	No	No
		1	PCSO	Improper disclosure of information	Local Resolution - by Division. No Action.	No	No
		1	PCSO	Improper disclosure of information	Local Resolution - by PSD. No Action.	No	No
		1	PCSO	Improper disclosure of information	No Action. Withdrawn - by Force.	No	No
		6	PCSO	Improper disclosure of information	No Case to Answer. No Action.	No	No
		1	PCSO	Improper disclosure of information	Withdrawn - by Force. No Action.	No	No
West Yorkshire Police	**58**	1	Police	Information not provided	Conviction	No	Yes
		6	Information not broken down	Accessing a police system for personal reasons	Disciplined internally	No	No
		5		Inappropriate disclosure of information	Disciplined internally	No	No
		1		Charged with sec 55 DPA	Disciplined internally	No	No
		1	Police	Information not provided	Resigned during disciplinary proceedings	Yes	No
		1	Police Support Staff	Information not provided	Resigned during disciplinary proceedings	Yes	No
		1	Police	Unidentified officer leaves paper file containing sensitive	None - Officer unidentified. Not	No	No

				data in raided property	reported to ICO		
		1	Civilian	Approved disclosure information had been applied to an application which was in fact information belonging to another applicant. This information was disclose by police staff employee.	Words of advice given. Reported to ICO.	No	No
		1	N/A	A technical issue on the computer database led to the accidental disclosure of information	System upgraded and the issue rectified. Reported to ICO	No	No
		1	Information not provided	Post Mortem report sent from Coroner's Office to wrong address	Words of advice given. Not reported to ICO.	No	No
		1	Police	Inappropriate comments made by unknown officer on NPT Twitter account	Dealt with at Division and content removed. Not reported to ICO.	No	No
		1	Police	Officer makes unauthorised disclosure to Service having assumed nominal's employment as notifiable.	Written apologies sent to complainant and to his employer. Reported to ICO.	No	No
		1	Information not provided	Refused under Section 40(2).	Management action. Not reported to ICO.	No	No
		1	Information not provided	OIC in requests partial medical records from victim's GP but receives full records. These are later sent to the defence team as unused evidence.	Advice given. Reported to ICO.	No	No

		1	Information not provided	WYP employee finds hardcopy email including victim personal details in litter bin	Advice given. Reported to ICO.	No	No
		1	Information not provided	Staff member on inadvertently sends wrong person details to practitioner under ISA arrangement.	Data had already been disclosed. Error noticed by recipient, correspondence deleted and WYP advised.	No	No
		1	Information not provided	OHU publish an anonymised Injury on Duty analysis spreadsheet on the Intranet. A fortnight later it is found that full personal details can be viewed via a "Data" tab on the toolbar.	Personal data removed. Not reported to ICO.	No	No
		1	Information not provided	Reviewing Officer inadvertently sends unredacted copy of employee's complaint concerning another employee to the wrong "Information" mailbox	Correct contact details to be circulated. Not reported to ICO.	No	No
		1	Civilian	Civilian Employee sends out Business Interests email to 30 employees but fails to use the bcc facility, resulting in advisory comment from one recipient	Advice given. Not reported to ICO.	No	No
		1	Civilian	Member of staff releases data to wrong email address. Reported	Recipient contacted immediately and requested to delete e-	No	No

				October 2013	mail.		
		1	Information not provided	Person alleges that custody record has been sent in error and a breach of data protection.	Dealt with at Divisional HR, management advice given. Not reported to ICO.	No	No
		1	Civilian	Members of staff release data to wrong email address. Individual notified by letter with explanation and apology. Reported November 2013	Advice given. Not reported to ICO.	No	No
		1	Civilian	Member of staff releases data to wrong email address. Individual notified the unit immediately stating that had opened but as soon as realised not for them deleted. Individual notified by letter with explanation and apology. Reported November 2013.	Advice given. Not reported to the ICO.	No	No
		1	Civilian	Member of staff releases data to wrong address. Identified when HR followed suit and sent a letter to wrong address.	Advice given. Not reported to the ICO.	No	No

		1	Information not provided	Complainant makes an anonymous report provided to solicitors and they have identified the complainant is the source of information.	Management action, words of advice given. Not reported to ICO.	No	No
		1	Police	Detention officer disclosed information to a third party requested a check about a friend.	Resigned. Not reported to ICO.	Yes	No
		1	Civilian	Member of staff releases data to wrong individuals e-mail address.	Advice given. Not reported to the ICO.	No	No
		1	Civilian	Members of staff release data to wrong HR cluster e-mail. Individual notified by letter with explanation and apology.	Advice given. Not reported to the ICO.	No	No
		1	Civilian	E-mail the Security Industry Authority for them to double check their register, included that the subject of the enquiry had been charged with an offence of on risk assessment was found to be non-disclosable	Advice given. Not reported to the ICO.	No	No
		1	Civilian	Member of staff e-mailed an ex-employee some manual payslips inadvertently emailed a number of other worksheets within that file	ICO referral management advice given to member of staff.	No	No

		1	Civilian	Whilst on a routine premises check a member of estates staff locates a box of paperwork in the kitchen area of location, upon inspection this is found to have personal information within it. Box is brought to Information Security and is stored in locked unit.	Box sent to storage. Not reported to ICO.	No	No
		1	Information not provided	Report was inadvertently sent to a Director within another Department.	Words of advice given. Not reported to ICO.	No	No
		1	Police	Police Constable informed a complainant, was in hospital. Whilst this matter was disclosed with the best of intention it does constitute a breach of the DPA in that sensitive personal data in the form of his physical wellbeing has been disclosed without his express consent.	Advice given. Reported to ICO.	No	No
		1	Information not provided	Blanket email sent to 43 x complainants linked to a crime, detailing a Crime Number. The email also displayed the current email addresses of all the other reciprocates.	Management action. Reported to ICO.	No	No

		1	Information not provided	Disclosure report sent via secure email to wrong partner agency.	Advice given. Not reported to ICO.	No	No
		1	Information not provided	Personal details in relation to a linked home address, were released to a local MP	Advice given. Not reported to ICO.	No	No
		1	Information not provided	Crime scene. Images had been sent to officers family	Final Written Warning. Not reported to ICO.	No	No
		1	Information not provided	Admin staff at sent a report to the wrong line manager.	Advice given. Not reported to ICO.	No	No
		1	PCSO	PCSO has disclosed information about to colleagues	Management advice. Not reported to ICO.	No	No
		1	Information not provided	OHU Information was released to line manager prior to the subject receiving the information	Information contained, management words of advice given. Not reported to ICO.	No	No
		1	Information not provided	OHU report regarding a member of staff was sent to the wrong HR Cluster.	Information contained, management words of advice given. Not reported to ICO.	No	No
		1	Information not provided	Report was accidentally sent out regarding an officer prior to its release date.	Staff member advised. Not reported to ICO.	No	No
		1	Information not provided	staff member reported that a report had accidentally been sent to the wrong HR.	Information contained, management words of advice given. Not reported to ICO.	No	No
		1	Information	OHU report sent to the wrong	Negative Pen Entry.	No	No

			not provided	HR mailbox	Not reported to ICO.		
		1	Information not provided	Staff member reported that they had accidentally sent a report to the wrong HR mailbox.	Negative Pen Entry. Not reported to ICO.	No	No
		1	Information not provided	Report sent to wrong department	Information contained, management words of advice given. Not reported to ICO.	No	No
		1	Information not provided	Staff member reported that a report was sent to HR in error	Advice given. Not reported to ICO.	No	No
Wiltshire Constabulary	**4**	1	Both	Data from all police forces from January 2012 was given to the NPIA (National Police Improvement Agency) to publish on the CrimeMapper website. Information sent by Wiltshire Police inadvertently contained some items of personal information. This information had come from a free text field in our STORM system, used to record reports made to the police. Approximately 62 data subjects had been affected and the data included names, ages, dates of birth, a mobile telephone number, a house number and vehicle registration numbers.	No formal disciplinary action - ICO informed	No	No

		1	Both	An asset audit was conducted by Wiltshire Police which identified the possible loss of devices containing personal data. The risk surrounding possible loss of data and the subsequent reputational risk was thought to be significant though it was not known what data was lost.	No formal disciplinary action - ICO informed	No	No
		1	Police	Email sent to incorrect recipient. The email contained the sensitive personal data of two suspects.	No formal disciplinary action - ICO informed	No	No
		1	Police	Two witness statements that were taken subsequently went missing	Ongoing. Reported to ICO.	No	No

Appendix 1: Methodology

A Freedom of Information request was sent to all UK police forces beginning on the 5th January 2016.

We asked for the number of times police officers and staff had been convicted, dismissed or disciplined internally for a data breach. In addition we asked for the number of employees that had resigned because of a data breach and those that hadn't received any disciplinary action.

We received a **95%** response rate. For the purposes of this report responses were included until 1st July 2016.

Appendix 2: Original Freedom of Information Request

Dear Sir or Madam

I am writing under the Freedom of Information Act 2000 to request information about breaches of the Data Protection Act 1998 in your police force, specifically I am requesting:

1. The number of a) Police officers and b) civilian employees that have been convicted for breaches of Data Protection Act 1998.
2. The number of a) Police officers and b) civilian employees that have had their employment terminated for breaches of the Data Protection Act 1998.
3. The number of a) Police officers and b) civilian employees that have been disciplined internally for breaches of the Data Protection Act 1998.
4. The number of a) Police officers and b) civilian employees that have resigned during disciplinary procedures 1998.
5. The number of instances where a breach has not led to any disciplinary action.

In each case, I request that you provide a list of the offences committed by the individual(s) in question, for example "*Accessed personal information for personal interest*" or "*Inappropriately shared victim information with a third party*".

I request that the time period covered is 1st June 2011-31st December 2015.

I further request that the information be displayed in the following format, I have provided the following examples for clarification:

Police/Civilian	**Outline of what was lost/reported missing/accessed**	**Data contained**	**Action taken criminal/ discipline**	**Additional responses to rectify loss**
Example: Civilian	Police USB stick lost.	Employee names, dates of birth and email addresses.	First written warning issued.	Additional training given.
Example: Police	Police laptop stolen.	Names of local residents who have reported a crime.	Suspended from work without pay for two weeks.	None - laptop encrypted.

My preferred format to receive this information is electronically, but if that is not possible I will accept hard copies.

I understand under the Freedom of Information Act that I am entitled to a response within twenty working days.

I would be grateful if you could confirm this request in writing as soon as possible.

About Big Brother Watch

Big Brother Watch was set up to challenge policies that threaten our privacy, freedoms and our civil liberties, and to expose the true scale of the surveillance state.

Founded in 2009, we have produced unique research exposing the erosion of civil liberties in the UK, looking at the dramatic expansion of surveillance powers, the growth of the database state and the misuse of personal information.

We campaign to give individuals more control over their personal data, and hold to account those who fail to respect our privacy, whether private companies, government departments or local authorities.

Protecting individual privacy and defending civil liberties, Big Brother Watch is a campaign group for the digital age.

If you are a journalist and you would like to contact Big Brother Watch, including outside office hours, please call +44 (0) 7505 448925 (24hrs). You can also email:

info@bigbrotherwatch.org.uk

For written enquiries:

Big Brother Watch

55 Tufton Street

London

SW1P 3QL

www.bigbrotherwatch.org.uk