Freedom of Information (FOI) request – IT Monitoring

Tranche 1 Force	Content of Force report	Page Number
City of London	The force cannot yet fully monitor all its IT systems because the software has limited capability and is not compatible with all the force's IT systems. This means the force must rely on audits of individual systems, which can be time-consuming.	37
Cumbria Police	The constabulary has good capability for monitoring its IT systems where it suspects there may be improper use. But this is confined to responding reactively to intelligence received. It could make greater use of its monitoring software to actively look for corruption risks. It could regularly check that officers and staff that have reported notifiable associations are not misusing systems.	41
Durham Police	We found very few intelligence reports relating to corruption. Most cases the counter-corruption unit investigated were reactive conduct issues. The low rate of reports of corruption has been questioned. The constabulary has responded to this by stating that it now has the ability to monitor all ICT systems. This is new to the constabulary since our last legitimacy inspection. Its use has not been fully implemented yet. There is some proactive use of ICT systems, as all incidents reported to the police are checked against force mobiles monthly in order to identify any issues that may suggest corruption. Over two years, this has not yielded any evidence of corruption.	42
Dyfed Powys Police	The force requires improvement in how it looks for and assesses intelligence about corruption. It regularly and consistently uses IT monitoring in its response to intelligence. But it makes only limited proactive use of its monitoring software. The software in use at the time of the inspection fieldwork did not extend to monitoring all mobile devices. So, the force cannot be confident that the workforce's use of data within its systems is appropriate and lawful. The software was extended to all mobile devices on 5 November 2018. While the force can now monitor all mobile devices, this will also bring additional work for the anti-corruption unit. The force needs to ensure sufficient capacity to undertake this important work	42
Essex Police	The force has made improvements in how it can identify such risks by acquiring new protective monitoring software. This is providing the force with the ability to assess, develop and deal with corruption-related intelligence. We are concerned that despite being able to audit some of its IT applications, the force is currently unable to monitor all its IT systems. However, the force is confident that it will soon be able to do so as it has recently purchased equipment to that end. We will revisit this area in future inspections.	44

Gloucestershire Police	The force is currently unable to monitor the use of all its ICT systems routinely. This creates a gap in its anti-corruption capability. The force recognises that it has technical problems in monitoring IT, but systems limitations make it unclear when this can be rectified. The CCU does have the capability to monitor open source and social media, which includes internet searches.	44
Greater Manchester Police	Although the force has invested in software which can be used to fully monitor all its IT systems, at the time of the inspection this was not being fully used. The force has assured us that, with the implementation of iOPS in early 2019, this issue will be resolved. But it remains a risk. The force currently uses its IT monitoring capability in criminal cases on the authorisation of a senior officer, rather than proactively looking for such data breaches. It makes decisions on the proportionality of monitoring in relation to any investigation and is not looking to change its approach. With full use of this technology, it could protect the data held within its systems and identify computer misuse.	49
Humberside Police	We found that the force doesn't yet have the capability to monitor all ICT systems and the data contained within them; this presents a risk to the force. The current system of auditing provides a large amount of data that is difficult to analyse, resulting in ineffective searches. The force is aware of both these matters and has plans to address them.	49
Kent Police	The new Athena IT platform should help the force to protect the information contained within its systems.	37
Leicester Police	The force has recently increased its technical ability to monitor the use of all force ICT applications.	45
Norfolk Police	We found that the force now has software to carry out real-time monitoring of its ICT systems, including those on mobile devices, besides its standard auditing capabilities. Testing of this monitoring software was being completed at the time of our fieldwork. This is being rolled out for all office-based hardware. Mobile devices are to follow in early 2019. The force is aware that live-time ICT monitoring could potentially increase the demand on the ACU, which has little scope to take on extra proactive work. The ACU's capacity was reviewed at the end of 2018 as part of the force's outcome-based budgeting process; agreement was reached to recruit into a vacant post. The head of the PSD and the deputy chief constable continue to closely and regularly monitor the effect on resources of ICT monitoring software.	39
Nottinghamshire Police	The force demonstrates a commitment to having the necessary arrangements in place to monitor its handheld and remote devices, so that it can check that officers and staff aren't misusing them. It moved to a new device-monitoring provider this year, which caused some technical problems with the existing security software. The provider has developed a solution, which it is currently testing before full monitoring resumes. In the meantime, the force is monitoring devices by auditing the individual systems.	44

West Midlands Police	Its capability to monitor computer systems continues to adapt to advances in technology, but it cannot yet fully monitor the use of all IT systems. New software is being bought that will enhance the unit's monitoring capability, but until this is in place this remains a gap for the force.	40
Wiltshire Police	Wiltshire Police identifies and manages internal corruption risks adequately. However, it conducts only limited monitoring of its ICT systems. This reduces its ability to identify and respond to corruption risks…… …The absence of monitoring presents a risk to information security. The force has evaluated commercial software products but hasn't yet identified a system that meets its monitoring needs. We will examine this facility again in future inspections. The force also needs to consider the capability and capacity of its CCU to review intelligence and move investigations forward.	41 and 42
Tranche 2 Force	**Content of Force report**	**Page Number**
Cheshire Police	The constabulary has invested in IT monitoring software. CCU staff are becoming increasingly experienced in using it. It was explained that this system can monitor all systems including hand-held devices and phones.	43
Dorset Police	Dorset Police has been a national leader in identifying and classifying intelligence about predatory behaviour and continues to develop work in this area. However, limitations in monitoring of IT systems means that it has not yet achieved our 2016 national recommendation that required all forces to implement a plan to achieve the capability and capacity required to address abuses of position. Neither is it clear that the CCU has the capacity to handle intelligence relating to abuse of position for sexual purpose. The force recognises this and is addressing resource levels in the department.	41
Hertfordshire Police	We saw that the force uses effective techniques to follow up intelligence and investigate cases. It also routinely monitors its workforce's use of data, including on mobile devices, for evidence of misuse.	43
Metropolitan Police	However, the way the force identifies potential 'internal insider threats' is only reactive. When it revised its borough intelligence units in 2014, it lost its local proactive capability to manage officers' activity. Dip-sampling individual use of ICT is no longer feasible and ICT monitoring systems are inadequate. Together with the high number of unvetted staff within the organisation, this leaves the force in a vulnerable position and is a significant organisational risk, because it cannot fully protect the information within its ICT systems. The force only responds reactively to the abuse of position for a sexual purpose. Its approach to ICT monitoring may be hindering this	59
North Yorkshire Police	The force doesn't have the capability to monitor all IT systems and the data contained within them. As a result, there are gaps in coverage. Recent extra capacity in the professional standards integrity unit is enabling the force to develop	45

	proactive processes to look for corruption linked to abuse of position for a sexual purpose by analysing data. But this is in its initial stages. The force should take steps to make sure that data is protected, and effective monitoring of technology can take place.	
Northamptonshire Police	The force has passive monitoring systems in place across almost all its ICT equipment. This includes the new mobile devices.	59
Northumbria Police	The force is now able to monitor some of its IT systems and the data contained within them to check that employees' use of data is appropriate and lawful, but it doesn't use this capability to proactively search for any inappropriate behaviour. The force has enough capacity and capability to address the current level of reactive enquiries and proceed to the investigation stage. IT monitoring went live in December 2018 and this should improve the capability to pursue corruption proactively that the force needs to focus on.	56
South Wales Police	At the time of our inspection, the force was not able to monitor all its IT systems. However, it is examining ways in which this could be done. Such a facility would mean it would be better equipped to make sure that all use of its data is lawful and appropriate. Further assessment may be needed by the force to make sure it maintains enough proactive capacity.	39
South Yorkshire Police	It takes early action to support members of its workforce who may be at risk of corruption. The force proactively monitors its information systems to identify corrupt behaviour and works with external organisations to help them to identify and report inappropriate and corrupt behaviour.	46
Suffolk Police	The force now has software for real-time monitoring of its ICT systems, including those on mobile devices, besides its standard auditing capabilities. This was being rolled out across the force. The force is aware that live-time ICT monitoring could potentially increase demand on the ACU, which has little scope to take on proactive work. The ACU's capacity was reviewed at the end of 2018, as part of the force's outcome-based budgeting process. Agreement was reached to fill a vacant post. The head of the PSD and deputy chief constable closely and regularly monitor the impact on resources of ICT monitoring software	42
Surrey Police	The force can't yet monitor all its IT systems. If it could it would be easier to check that officers and staff aren't misusing them. The force is fully aware of this and is working to solve this problem. The specialist teams that look for and tackle corruption have enough staff and resources.	41
Thames Valley Police	At the time of the inspection, the force couldn't fully monitor all its IT systems to identify potentially corrupt use. The force has told us that it will resolve this issue during 2019. In collaboration with the Hampshire Constabulary, it has	41

	purchased software that (from March 2019) will allow it to monitor the use of force IT systems by employees who are suspected of involvement in corrupt activity. This will be upgraded later in the year to allow overall continual monitoring of all force systems.	
Warwickshire Police	Due to the current IT infrastructure, the force cannot monitor some of its IT systems. But it has approved a business case and set aside funds to enable this monitoring when infrastructure improvements allow. The ACU has a good understanding of its auditing capability. An ACU analyst is developing a proactive approach to the analysis of ICT systems, so that the force can identify officers and staff who may pose a risk of corruption. The absence of technical solutions to monitoring means that the force is very reliant on limited ACU analytical capacity.	63
West Mercia Police	Due to ICT infrastructure problems, the force cannot yet fully monitor all its ICT systems. However, it has approved a business case and set aside funds to purchase such a system when infrastructure improvements allow. In the meantime, the PSD has completed a list of the auditing capability of the force. The ACU has a good understanding of its auditing capability. An ACU analyst is developing a proactive approach to the analysis of ICT systems, so the force can identify officers and staff who may pose a risk of corruption. This means that currently the force is very reliant on limited ACU analytical capacity in the absence of other technical solutions.	64
Cleveland Police	The force has invested in monitoring software, but staff were trained so long ago that they are no longer confident in using it. The software also has some limitations because it can't monitor all the force's IT systems.	58

Tranche 3 force reports are not yet published.