HMCPSI
HM Crown Prosecution Service Inspectorate

Inspection of CPS information management

A review of the CPS's controls to manage case information

October 2020

If you ask us, we can provide this report in Braille, large print or in languages other than English.

For information or for more copies of this report, please contact us on 020 7210 1160, or go to our website: justiceinspectorates.gov.uk/hmcpsi

HMCPSI Publication No. CP001: 1276

Who we are

HM Crown Prosecution Service Inspectorate inspects prosecution services, providing evidence to make the prosecution process better and more accountable.

We have a statutory duty to inspect the work of the Crown Prosecution Service and Serious Fraud Office. By special arrangement, we also share our expertise with other prosecution services in the UK and overseas.

We are independent of the organisations we inspect, and our methods of gathering evidence and reporting are open and transparent. We do not judge or enforce; we inform prosecution services' strategies and activities by presenting evidence of good practice and issues to address. Independent inspections like these help to maintain trust in the prosecution process.

Contents

Annexes

1. Summary

Background and context

1.1. Over recent years it is fair to say that the Crown Prosecution Service (CPS) has been at the forefront of modernising the criminal justice system – in particular, digitising its internal and external processes. Paper and hard media are things of the past, having been mostly replaced by digital systems. Case material is dealt with from cradle to grave digitally. This has helped ensure efficiency and increase security.

1.2. Concerns have been raised in recent internal audits around the significant amount of security breaches – and in turn, the volume of self-referrals to the Information Commissioner's Office – by the CPS. On two occasions, this has resulted in fines being imposed.

1.3. There is much more public awareness of data security and this, in turn, has resulted in more emphasis on information management across public bodies. The general public want and deserve reassurance that their information and personal data is being handled safely and correctly. The CPS, like other public sector bodies, has a responsibility to have robust systems in place to control and manage its data handling, given the sensitive case information it handles on a daily basis.

1.4. To review all aspects of information management in the CPS with the resources available to the Inspectorate would be impossible. A decision was made to focus the inspection on a series of objectives, with evidence gathered to support the assessment by examining a file sample of cases from across the 14 geographic CPS Areas. The four objectives are set out in the inspection framework in annex A.

1.5. This report must be read with an understanding of the police's responsibilities with regards to information management. In effect, all criminal cases start life with the police. The police generate the casefile as a result of their investigation and submit digital material to the CPS in line with the National File Standard appropriate to all forces in England and Wales. Material and information are sent to the CPS at various stages of the process.

1.6. When the casefile is digitally transmitted to the CPS, the CPS becomes the owner of that information. If the CPS then sends or transmits information provided by the police on to other agencies, it becomes entirely responsible for what is dispatched at that point.

1.7. The role the police play is critical. There are rules of evidence to support criminal investigations. All officers are provided with guidance and training to

make sure that case material is produced in line with the expected standards of data protection. Names, addresses and phone numbers should only be included in statements or case summaries if they are key evidence and officers should be aware of their obligations.

1.8. Our findings in this inspection highlight that there is a serious lack of awareness and compliance by front line police officers. The majority of the data breaches the CPS made were the result of information being included in material that the police sent.

The CPS deals with incredibly sensitive information on a daily basis

1.9. It is often fortunate that the CPS, which rightly has the responsibility to ensure that personal data is not transmitted incorrectly, acts as a 'backstop': examining police-generated material before it is sent out.

1.10. While this report can only focus on the CPS and the concerns over security breaches stemming from the service of papers, it should be read with the understanding that the mistakes that lead to breaches in the files we examined in the main originated from the police. This is something the CPS is aware of, feeds back on regularly, and is having ongoing discussions with the police about.

1.11. The CPS deals with incredibly sensitive information on a daily basis, from the name of a shop that has been targeted for theft to the names and addresses of complainants in rape cases. The information it possesses is subject to the rules and regulations of data protection and all staff have a responsibility to make sure documents are processed securely and in line with data security requirements.

1.12. The information received from the police needs to be transmitted to others – be that to the defendant themselves, their representative, or the court – to allow others to access the correct material to ensure that justice is done.

1.13. Information received from the police may need to be dealt with very quickly. In overnight custody cases, the defence and the court need to have the information before the court starts; this means that the CPS must deal with the casework information under pressurised timescales. However, the CPS has a duty to the public to ensure that it always deals with that material in a secure way. In line with data protection guidance, the CPS becomes the information asset owners at the point of receipt of the information from the police.

1.14. What this report seeks to understand is whether the CPS has the right processes and systems in place to manage casework information. Simply put,

this report sets out our findings against the inspection question "Does the CPS have suitable controls in place to ensure that case information is managed securely and appropriately?"

1.15. This report does not seek to make judgments about every aspect of information management within the CPS. It focuses primarily on the security of documents sent by the CPS to others. We have also limited our inspection to the first stage of cases in the magistrates' courts. As part of the inspection, we examined 700 cases (50 from each CPS Area) to look at how effectively the CPS deals with cases before the first hearing in the magistrates' courts. We also looked at the level of training provided to staff and how the CPS deals with breaches and security issues.

Key findings

File examination

1.16. In 98 of the 700 cases we examined (14%), information was passed on to the CPS that should have been either redacted or not included. Simply put, this amounts to 14% of cases containing a security breach. The CPS was able to prevent breaches in 10 of those cases, meaning that there was a breach in 12.5% of all cases we examined. Given the nature of the work the CPS undertakes and the information being handled, this level of breach is unacceptable.

1.17. In 60 cases (61%), the breach was the result of unauthorised disclosure of information included in the body of a witness statement. In some cases, personal information is required to be able to prove an offence – for example, an address in a burglary offence – but otherwise, even where known to a defendant, personal information should not be disclosed. In these cases, personal data was shared with others where it was not required to prove the case. In all cases, these statements were provided to the CPS by the police and the inclusion of the personal data within the body of the statement was initiated by the police.

1.18. The other 38 breaches (39%) included a range of errors. Some of these involved CPS staff sending the wrong set of previous convictions – that is, those not intended for the defence or the court. In some, the case summary contained an unauthorised disclosure. Witnesses' personal details are recorded on the backs of witness statements so they can be separated from the body of the statement, reducing the risk of forward transmission – but in some cases, the back of the witness statement was included in the documents shared. Other examples included the service of exhibits containing the victim's medical notes unredacted, injury photographs of the victim showing their date of birth on a

hospital wrist band, and service of the wrong case summary – that is, a summary that related to a different case entirely.

1.19. It is not for our inspectors to assess the risk level of a breach; our assessment is whether there was evidence of a breach in the cases we examined. In some cases, whilst the inclusion of the incorrect information was an error in terms of data protection and information security, it did not amount to a breach of such magnitude that it should have been reported to the Information Commissioner's Office. There were a few examples, however, where inspectors felt that the breach was of such consequence that it may have resulted in an increased risk and as such should have been reported. We shared all case references where inspectors identified a breach with the CPS to allow it to assess the risk and decide whether to report it to the Information Commissioner, and to allow feedback to be shared with the police.

Policy, training, support and reporting breaches

1.20. Whilst the CPS has developed a considerable amount of policy and guidance to support information management generally, our findings show that there is a lack of clarity and understanding at the operational level in relation to handling casefile material.

1.21. Those staff that did know of the national policies and where to find them said they often found them complex and difficult to navigate, and that they did not directly relate to their role in handling casework material. Staff generally also only accessed policy as a reactive or retrospective action when something had gone wrong or as a result of a breach.

1.22. Staff at all grades were aware and understood that all casework material should be checked to determine whether it needs to be redacted before being sent out or forwarded to others in the criminal justice system. However, there is a lack of consistent national guidance to help staff determine what does and does not need to be redacted from casefile material. Inspectors understand that producing specific guidance is not straightforward; for example, it is not as simple as saying that all addresses should be redacted, because in some cases addresses should be included in statements, such as in the case of a burglary. Staff regularly indicated that some clear principles on what should be redacted would be helpful, and some nationally produced training around the specific issues in casefile material for operational staff would also help establish a consistent approach.

1.23. Measures have been put in place recently to improve training and understanding amongst all staff. Significant activity has focused on the CPS intranet to highlight data security and individual responsibilities in information

management. The Inspectorate acknowledges that these recent attempts to engage staff and improve awareness of information management – the publicity campaign, events and supporting documentation – are being given a very high degree of prominence and are engaging. The simple message of 'The BIG Tidy Up' was resonating with some staff – even though the campaign had just commenced as we were finalising Area interviews.

1.24. There are processes in place to log and record both redactions and security breaches. The redaction logs capture the cases where CPS staff have redacted sensitive information from material before serving it on others in the criminal justice system. The security breach logs record breaches where unauthorised disclosure of information has occurred in material served by the CPS.

1.25. Whilst all staff clearly understood the need to check and redact documents where appropriate, there was a lack of clarity in some Areas about the process, including whether redacting material and logging redactions fell to operational delivery or legal staff. Some legal staff said they would rarely log any redactions. This can lead to the scale of the problem being masked. Consequently, the information shared with the police is not always an accurate reflection of the level of redaction and rework required.

1.26. Some of this reluctance to log redactions was a result of the view that performance would not improve no matter what action was taken by the CPS, because the continual feedback of these issues to most local police forces had not resulted in any discernible improvement.

1.27. The process around logging security breaches serves two purposes:

- for audit purposes, in case there is a need for the Information Commissioner's Office to be involved
- to allow the Area to feed back to the police when the initial issue is something they transmitted that should have been redacted or not included at all.

1.28. There is general awareness that staff should report breaches to line managers, but the only clearly defined national process is for security breaches to be reported to the Security Information Assurance Division (SIAD) within 24 hours on the approved form. Internal processes within some Areas are less clearly defined, and inconsistencies can occur resulting in breaches not being properly recorded or reported to either SIAD or the police.

1.29. Inspectors were told by senior managers that the local relationships with the police were such that both the redaction and security breach logs were

shared, but there was very limited evidence to point to any performance improvement.

1.30. Given the level of breaches identified in our case sample, it is somewhat surprising that there is no formal quality check or assurance process to support the identification and logging of breaches. Some established quality assurance systems might identify cases when there is a manager check – for instance, in individual quality assessments, which are retrospective assessments of a lawyer's work – but there were no formal checks performed in any of the Areas we visited. Other general compliance and management checks may also pick up issues in work carried out by operational delivery staff, but again, these are sporadic and not specifically focused on identifying or effectively logging breaches.

1.31. Given the impact and seriousness of sending out the wrong information, either because it is not redacted or because the individual member of staff has made a genuine mistake, there need to be clear expectations of how staff are to be dealt with when a breach occurs. In some Areas, we were told that staff could make up to five breaches before they needed to undergo further training. This seems to highlight a culture where it is acceptable to make breaches and any consequences are limited. We also found inconsistency in how staff were treated with regard to the application of the CPS's performance management policy.

1.32. There appears to be a culture of defeated acceptance that no matter what training, processes and systems are introduced, there will always be breaches, with data that should have been redacted being sent out, because of what is received from the police. Given the extent of the breaches we identified, it is difficult to counter this view, but the CPS need to ensure that it works effectively with partners to reduce the propensity of the risk, that its internal processes and systems are effective, and that the organisational culture changes to look on data breaches as a critical failure.

Recommendations and good practice

Recommendations
The Crown Prosecution Service should develop consistent principles and guidance, for both operational delivery staff and legal staff, around information management when handling casework material, and make sure these are implemented in all Areas. Guidance should be developed that includes both clarity about what constitutes a security breach in case material and principles to determine what material should be redacted. (paragraph 4.13)
The Facilities, Estates and Security Manager role should be reviewed. The review should clarify the skills and experience required by the role holder and set out, with clarity, the responsibilities around information management, particularly around logging and quality assurance in case material handling. (paragraph 4.17)
A bespoke quality assurance check or process should be implemented to support the identification and logging of redactions and security breaches. (paragraph 5.17)
A consistent process for logging redactions and security breaches should be defined and implemented in all Areas to ensure the consistency and accuracy of data. (paragraph 5.23)
The Crown Prosecution Service should develop bespoke training modules for operational delivery staff and legal staff in Areas, defining roles and responsibilities in handling casework material and processes around logging redactions and breaches. This training should be mandatory for all Area staff and a record of completion should be retained and returned to Crown Prosecution Service Headquarters. This should also be a mandatory part of induction for staff in all roles. (paragraph 6.15)
Performance data around volumes of redactions and security breaches, both locally and nationally, should form part of the Crown Prosecution Service's data pack, to raise awareness amongst all staff and to make sure Areas are accountable for their performance in this aspect of work. This information should form part of the performance data discussed at Area Performance Reviews. (paragraph 7.10)

Good practice
A monthly poster informed staff about the latest performance figures and any recent policy changes or 'need to know' information. Staff were positive about how this raised the profile of information management and allowed them to clearly understand current issues. (paragraph 6.16)

2. Framework and methodology

Inspection question

1.33. Our inspection question was: “Does the Crown Prosecution Service (CPS) have suitable controls in place to ensure that case information is managed securely and appropriately?”

1.34. In order to answer this question, our inspection framework (set out in full in annex A) was divided into four areas:

- policy and guidance: does the CPS have a clear policy available and disseminated to all on the management of information?
- internal management of casework: does the CPS have effective controls and measures in place to ensure information shared is secure and appropriately managed?
- training: does the CPS have suitable knowledge and training resources to ensure the organisation understands information management?
- security breaches: is the CPS effective in dealing with security breaches and future proofing information management risk?

How we inspected

1.35. We examined 700 files (50 cases from each of the 14 CPS Areas) and used a set of questions to assess the nature and frequency of security breaches. We chose a combination of live and dead files, focusing on the ‘initial details of the prosecution case’ bundle sent out to court and the defence. This bundle includes the key evidence in the case, including a case summary provided by the police and any key witness statements. As all cases start with a hearing in the magistrates’ court, this file sample included cases that would be heard in magistrates’ courts and the Crown court.

1.36. The file examination provided us with statistical data, set out in chapter 3. The bespoke set of questions we used can be found in annex B.

1.37. We reviewed policy, guidance and training materials on information management. To assess the quality and effectiveness of material at the national and Area levels, we looked at:

- the national intranet
- Areas' local intranet hubs
- operational delivery material
- material generated and provided by Areas.

1.38. We considered whether the CPS was following its policy in terms of case information and sharing material. In particular, we considered how Areas were delivering and interpreting the policy.

1.39. We conducted interviews virtually at the Area and national level, using Microsoft Teams because of the coronavirus pandemic. We 'visited' five Areas, interviewing the Area Business Manager, legal and operational delivery managers, Facilities, Estates and Security Manager (FESM), and focus groups of operational delivery staff and crown prosecutors in each one.

1.40. In CPS Headquarters, we interviewed senior members of staff including the Head of the Security and Information Assurance Division, the chair and a member of the Audit and Risk Committee, the Director of Finance and the Director of Operations, Digital and Commercial.

1.41. Through a combination of file examination, document analysis, and interviews, we were able reach an evidence based assessment of how well the CPS manages case information against the four framework questions.

3. File examination and data analysis

As set out in chapter 2, we examined 700 files from 14 different Crown Prosecution Service (CPS) Areas, answering the file assessment question set. This established what type of case we were examining and, most importantly, whether there had been a security breach. This involved looking at all documents within a case up to the service of the initial disclosure of the prosecution case (IDPC) bundle at the first hearing.

We sought to establish whether material was included in the IDPC and sent to parties in the case that should not have been; if so, what the nature of that material was; and whether the CPS had identified and addressed it before serving the case material on other parties within the criminal justice system.

Overall all Area findings

Question	Answer	All cases	CPS responsible
All cases			
Has there been a security breach?	Yes No	98 (14%) 602 (86%)	88 (12.5%) 612 (87.5%)
Type of breach (of the 98 cases where a breach was identified)			
Unauthorised disclosure in a case summary	Yes No	19 (19.4%) 79 (80.6%)	16 82
Unauthorised disclosure in a witness statement	Yes No	60 (61.2%) 38 (38.8%)	54 44
Back of witness statement included in bundle	Yes No	3 (3.1%) 95 (96.9%)	3 95
Incorrect media links of content sent	Yes No	0 (0%) 98 (100%)	0 98
Incorrect set of previous convictions sent	Yes No	11 (11.2%) 87 (88.8%)	11 87
IDPC dispatched to incorrect email address	Yes No	98 (100%) 0 (0%)	98 0
Other type of breach	Yes No	18 (18.4%) 80 (81.6%)	17 81
Identification			
Did the CPS identify and rectify all breaches sent in by the police?	Yes No	10 (10.4%) 86 (89.6%)	

1.42. Our file examination established that most security breaches occurred from material sent over by the police that should have been redacted. In the main, this occurred by way of unauthorised disclosure in witness statements (61%) followed by unauthorised disclosure in case summaries (19.4%).

1.43. There were no examples of breaches occurring by sending the bundle out to the wrong email address or sending out an incorrect media link (to access digital media such as CCTV or body worn video footage).

1.44. It is of note that, while we found 98 security breaches in our file examination, the CPS was able to identify and rectify breaches in 10 of those cases. Therefore 88 cases (12.5%) contained a security breach sent out by the CPS.

1.45. The category of 'other' breaches is significant enough to mention and gives an idea of the potentially serious nature of some of the breaches. Examples included the following.

- A doctor who examined the victim provided a statement, to which a fee note was attached that set out the doctor's home address.
- An exhibited photograph was sent out depicting a victim wearing a hospital identification wristband, on which the victim's date of birth was clearly visible.
- A case summary pertaining to an unrelated case (one with a different defendant) sent in by the police was sent out to the parties in another case entirely.
- A schedule listing non-sensitive unused material (that is, material not used as evidence by the prosecution but which has been collated during the course of the investigation), which was sent out alongside the IDPC, contained the name of the neighbour who had called the police. This had been redacted from the witness statement in the IDPC, but remained unredacted in the schedule.
- Medical discharge notes were exhibited which included personal details of the victim, including address, phone number, date of birth, NHS number and GP details.

1.46. We also looked at how effective the CPS was in identifying and rectifying any issues before they served the case material, and so preventing a security breach.

1.47. In ten cases where there were issues with the case material, the CPS identified and addressed the issues before the IDPC was served, thus preventing a security breach. In the remaining 86 cases, the issues were not identified and so went on to become security breaches.

1.48. The concern is that if CPS staff are not able to identify what needs to be redacted or amended in case material before it is served, they will not be able to identify when a security breach has occurred, because this requires the application of the same principles. As we found no evidence of specific quality assurance measures around the identification and recording of security breaches, it is apparent that Areas rely on staff to identify and record them. There is therefore a concern that the volume of security breaches logged and recorded is inaccurate.

1.49. We looked at 50 cases in each CPS Area. The table below outlines how many security breaches we found in the cases we examined.

Area	Breaches
Merseyside & Cheshire	16
Eastern	12
Wales	11
East Midlands	10
North East	10
South West	8
West Midlands	6
North West	6
Wessex	4
South East	3
Yorkshire & Humberside	3
London North	3
Thames & Chiltern	2
London South	2

1.50. In five of the 14 Areas, there were security breaches in 20% or more of the cases we examined.

4. Policy and guidance

1.51. There is no single overarching Crown Prosecution Service (CPS) policy document on information management. Policies and guidance set out the CPS's overarching rules on specific aspects of its work. For example, the policy on data breaches outlines how the CPS will comply with data protection legislation and what is expected of employees.

1.52. Overall, information management policy is made up of a collection of documents that are available on the Security Information Assurance Division (SIAD) website. The main policy documents relate to data breaches and document retention.

Areas have a general awareness of information management policy, but there was confusion about the specifics of policy and where it is held

1.53. In interviews with us, many staff indicated that it was difficult to locate a specific policy or guidance to assist them in relation to operational matters affecting their role.

1.54. The SIAD is aware of the large number of separate documents and is making attempts to combine these into a more simple and accessible series of documents. It has created a policy review board tasked with reviewing and rationalising all national and local policy documents.

1.55. We found that Areas have a general awareness of information management policy. However, at almost all grades of staff, there was confusion about the specifics of policy and where it is held. When asked about what policies the CPS has around information management, most operational staff referenced the General Data Protection Regulation (GDPR) but were less clear about the application of information management to their specific roles.

1.56. Those that did know of policy and where to find it said that they often found the relevant pages on the CPS intranet complex and difficult to navigate in order to locate specific information. Staff generally only accessed policy as a reactive or retrospective action, to determine what steps they should take after a problem had been reported or an error identified.

Awareness of the Security Information and Assurance Division

1.57. One of the main communication tools used by the SIAD is its Info-net page on the internal CPS website. A recently published Information Commissioner's Office (ICO) report noted this was an area that needed improvement.

1.58. Given the timing of the on-site interviews, which we conducted before a large number of recent intranet articles were published, we found almost universally that few staff other than senior managers knew about the SIAD or what it does. We did note a change towards the end of our inspection because of the recent intranet activity.

1.59. The Head of SIAD told us that they are working with the CPS's communications department to continue and develop this proactive communication. This is part of an ongoing strategy to raise the profile of data security and its importance. During the inspection we certainly noticed the higher profile of activity on the CPS intranet. This included messages around home working, a new training course and a data awareness campaign called The Big Tidy Up that aimed to inform staff about data retention policy.

1.60. We found that, even during the relatively short period of our inspection, improvements have been made and there has been a concerted effort to raise the profile of the team, its role, individual staff responsibilities for data security, and the focus on data security. There is a lot of information available on the intranet, as well as links to further content. The feedback we received in Area interviews was that more thought could be given to basic signposting of what the teams in security do and the different roles that are there to support staff. In our view, the proactive focus on data security should help raise awareness which, given the findings of this inspection, is a step in the right direction.

Policy delivery

1.61. From our file examination and interviews across the Areas, we found little evidence of a national or consistent approach to training to support information management policy, other than some basic national GDPR training which took place more than two years ago. Many staff we spoke to indicated that that was their most recent training on anything specific to information management. On 1 July 2020, the CPS introduced a new data protection training package.

1.62. We found most Areas had produced local guidance because of what they had identified as a gap in turning national policy into operational guidance for Area staff handling case material. This has led to inconsistent processes and approaches developing in Areas, some of which are clearly out of date. When we requested documents from Areas to support their approach to information management, some Areas produced documents dating back as far as 2015 and staff in interviews often referred to old Area guidance.

1.63. It is understandable that, in the perceived absence of clear national guidance, Areas have developed local guidance. But it is questionable whether, in the context of a national organisation with Standard Operating Practices, that local guidance should exist. This is something the SIAD indicated it would be considering as part of its review of policy and guidance documents.

Recommendation
The Crown Prosecution Service should develop consistent principles and guidance, for both operational delivery staff and legal staff, around information management when handling casework material, and make sure these are implemented in all Areas. Guidance should be developed that includes both clarity about what constitutes a security breach in case material and principles to determine what material should be redacted.

1.64. It appears that the main method of delivering policy or guidance on information management at the Area level is via an individual member of staff: the Facilities, Estates and Security Manager (FESM). This is a member of the team with responsibility for the facilities, estate, and security of that specific Area. The policy delivery approach appears to be for FESMs to present information to managers, and managers to then cascade it to staff.

1.65. This means that CPS Headquarters and Areas are reliant on having a competent and efficient FESM who can effectively engage and deliver training, support and key messages. There is a risk that this may result in an inconsistent message to staff – for example, if the message is not understood by managers or diluted in onward delivery. There is also the risk that national messages may be delivered differently from Area to Area. We found that FESMs' level of

casework experience differs greatly, which affects their ability to translate policy into effective guidance at operational level.

1.66. During interviews with senior managers in CPS Headquarters, it was apparent that the scope and scale of FESMs' responsibilities are already being considered. It was noted that more clarity is required about FESMs' roles, responsibilities and accountability at the national and Area level. It was also accepted that there is a need for much more focus, at a local level, on data security and management, and that more resources are needed if the management and control of data are to be improved. Managers and FESMs we spoke with in Areas generally felt the role was too big, and in some places there was a recognition that some of those in the role lack consistency and experience.

1.67. In some Area interviews, it became clear that seeing the FESM as being responsible for data and data security issues dilutes the message that information management is everyone's responsibility. The FESM, perhaps largely because of the "Security Manager" part of the job title, was seen as the person who ultimately had everything to do with all information management and, as such, who would deal with all issues within their Area. Whilst this was indeed the case in some Areas, this is not universal, and our inspections point to a risk of the FESM role undermining the position that information management is everyone's responsibility. In some Areas we visited where the FESM focused on other aspects of the role, taking only a very minor role in information management, staff did not refer to the FESM except to note that they oversaw the process to report breaches.

Recommendation
The Facilities, Estates and Security Manager role should be reviewed. The review should clarify the skills and experience required by the role holder and set out, with clarity, the responsibilities around information management, particularly around logging and quality assurance in case material handling.

1.68. Many staff were vague about whether they had been trained on a specific CPS information management policy, other than some GDPR training which took place some time ago. Staff did accept that weekly local newsletters and national gateways contained information to support data security, although it seems the effectiveness of this as a means of communication was limited. In many cases, it seemed that staff referred to policy and accessed guidance when something had gone wrong, often after a breach had occurred. This appears to have driven a largely reactive approach, accepting security breaches as inevitable, as opposed to a proactive one targeted at preventing security breaches from occurring in the first place.

Compliance monitoring

1.69. Areas monitor their local performance, in terms of the level of breaches reported and data security instances, through quarterly Area Performance Reviews. These reviews consist of CPS Headquarters staff reviewing an Area's performance against set criteria, which include information management. The SIAD also uses other methods to keep track of policy awareness and to monitor performance. These include:

- quarterly breakdowns of the Area's main security incidents
- a monthly metrics report spanning all instances the SIAD has dealt with
- a breakdown of specific Area performance by the Departmental Security Unit, including some evidence from the results of targeted deep dive exercises, where there has been a more extensive analysis in an Area
- training compliance data.

1.70. There was evidence of an appreciation of the importance of information management to the organisation at a strategic level. This was evidenced throughout the inspection, with Areas talking about information management in their Area Performance Reviews. We were also made aware that information management is now a standing agenda item for the Audit and Risk Committee, with the Head of SIAD reporting directly to the committee. Our interview with the CPS's Finance Director discussed the big risks to the CPS: currently, two of the top ten organisational risks relate to data management.

1.71. The Head of SIAD has accepted the need to maintain the policy message. One interviewee said that "Chief Crown Prosecutors will recognise that they are the information asset owners and they should be leading by example". Information management has perhaps not been given the "prominence that it should have" but the CPS as an organisation is trying to change that.

1.72. In September 2020, training for Chief Crown Prosecutors (CCPs) will start. There is also a plan to include information management as a performance objective for several senior grades (we were told this would include CCPs). There is the potential to roll out information management performance objectives to all staff in the future.

1.73. From an Area perspective, staff see their awareness of policy and practice as coming from e-learning, local guidance, and team meetings. The maintenance and monitoring of policy within Areas appears to be very much left to FESMs or operational delivery managers.

5. Internal management of casework

Clear process

1.74. The Crown Prosecution Service (CPS) receives case material from the police. This material, collated during the investigation, is reviewed by the CPS and either shared as evidence or listed on an unused material schedule. Any material that the CPS intends to rely upon as evidence is then shared or served on the other parties: usually the court and either a defendant in person or their solicitor. Anything that is shared or served on other parties is referred to as shared case material.

1.75. Those we interviewed were all aware of the policy that "all shared case material should be checked before dispatch to ensure all materials are suitable for disclosure". This understanding has been largely driven by the introduction of the General Data Protection Regulation (GDPR) several years ago, but has been maintained by managers and by the general day to day duties of most staff who have to deal with sensitive information.

1.76. There was also evidence that all Areas have some processes in place to manage shared case materials, largely based on the CPS's Standard Operating Practices.

1.77. The findings from this inspection show that in most cases (86%), the case material contains no sensitive material that requires redaction. There was also evidence that the redaction of sensitive information does take place; those interviewed were able to identify common problems with police files and give examples of when they have had to redact documents. They were also able to show that some information about redaction (such as the type and volume of redactions) is shared with the police, albeit not consistently. This tends to be in the form of logs kept by Areas.

1.78. However, interviews with staff highlighted issues around the detail of what should be redacted from documents, by whom and at what stage. In some Areas, legal staff were unaware that operational delivery staff checked all documents before the prosecutor. There were also inconsistencies around whether material should be returned to the police to redact if there was time to do so, or whether CPS staff should do it. Many legal staff indicated that they did not know how to redact a document themselves and so would set a task for an operational delivery colleague to do it.

1.79. All Areas keep a log of redactions that they have completed and material that has been sent back for the police to redact. Area Business Managers should share these logs with Chief Constables of local police forces as a driver for improvement by the police.

1.80. Although all Areas had a log, completion of the log was inconsistent. In most Areas, interviews highlighted that operational delivery staff were mostly and consistently logging redactions; but in many Areas, legal staff indicated they may redact material but not put it on the log. This appeared to be the result of various factors, including:

- a lack of knowledge about the need to do this
- a lack of knowledge about why the Area collated the information
- a lack of time
- a perception that, despite the collation of this information over a significant period of time, no discernible improvement has been seen in the material received from the police.

1.81. The impact of this is that the information shared with the police is not always an accurate reflection of the level of redaction required.

1.82. All the Areas we inspected indicated in interviews that there is no national guidance on what to redact. Our findings are that this has led to ambiguity and inconsistency across Areas. Some Areas have drawn up local guidance on what to redact; others have left the judgment of whether a piece of information requires redaction up to the individual responsible for checking the documents. In many cases this is an operational delivery member of staff with no legal qualifications or legal training. In all Areas, however, staff did indicate that they were able to consult with colleagues or managers to assist with these decisions, where time allowed.

1.83. Operational delivery staff also highlighted an anomaly in the process for CPS charged cases. Where a CPS prosecutor is asked to provide advice on charge, if the decision is to charge the suspect(s), the documents should be checked by the prosecutor making the decision to charge. They should either redact the material themselves or provide instructions to operational staff. Staff told us in interviews that CPS Direct prosecutors do not do this, which creates a risk in overnight cases, where there is no lawyer review before dispatching the initial details of the prosecution case bundle. Checking these sometimes complex and voluminous cases is left to a member of operational delivery staff, operating under significant time pressures. This is an aspect that the CPS may wish to consider in terms of risk.

1.84. All those interviewed indicated that they would welcome national guidance to assist in achieving consistency in redaction. They accepted that a definitive list would not be possible, given that certain sensitive information must be kept in case material where it is required to prove the case, such as an

address in a burglary offence. One suggestion was to draw up a set of guiding principles, which could include common exceptions, such as addresses in burglary cases and dates of birth for certain sexual offences.

Compliance

1.85. In all the Areas we inspected, we saw some evidence of processes for recording and monitoring redactions and security breaches. However, the interviews we conducted with Area staff highlighted that not all breaches were being identified, because not all staff (mainly lawyers) recorded cases where material had to be redacted or highlighted a breach.

1.86. CPS Headquarters expects Area Business Managers to forward spreadsheets and information to Chief Constables, setting out where the police have not properly redacted case material sent to the CPS. Most Areas share this information, but not always at Chief Constable level; in some Areas, this has been delegated to lower ranks within the police, such as Inspector level. We found very limited evidence that logging and sharing this information has driven any real improvement, in terms of reducing the amount of sensitive material received from the police in case material.

1.87. Areas reported that there is no formal requirement for any assurance work to take place to make sure redactions have been identified, addressed and logged. Consequently, inspectors found significant variance. Some Areas have a requirement for a percentage of the documents they send out to be checked; some undertake ad hoc spot checks; others cited manager checks, such as individual quality assessments and lawyer appraisals, as methods that would also identify information management issues. Other Areas indicated that no checks took place at all.

1.88. We were told that in South East and Wessex, some assurance takes place in the form of weekly dip samples. These two Areas had the second and third lowest numbers of security breaches across the Areas inspected in our file examination. The South East file sample had three breaches (6%) and the Wessex sample had four (8%).

1.89. Merseyside & Cheshire had 16, the highest number of breaches (32%). In this the Area, the redaction logs are shared at Inspector level with Cheshire Police and at Superintendent level with Merseyside Police. The performance in Merseyside & Cheshire may be a coincidence, but the facts that this Area had the highest level of breaches in our examination and that there is limited effective engagement with the police at a senior level may point to an issue that needs urgent attention.

1.90. We found evidence that Areas complete a quarterly assurance and a risk register, which are sent to CPS Headquarters. This includes some information management aspects, although in the absence of any bespoke quality assurance work, we have concerns about the effective assessment of risk based upon these returns.

Recommendation
A bespoke quality assurance check or process should be implemented to support the identification and logging of redactions and security breaches.

Roles and responsibilities

1.91. All the staff we interviewed were clear that they were responsible for the information they dispatched. There was real appreciation of the importance of ensuring information was properly checked and redacted before sharing with other parties, and of the impact on individuals whose information was inappropriately shared.

1.92. Most cited that the police have the initial responsibility, but that once the material is passed to the CPS, it falls to them to take responsibility. In some Areas, there was a sense of frustration that the police passed the responsibility to the CPS, as well as with the perceived imbalance in the relationship and that any activity to address it with the police is generally ineffective.

1.93. Staff expressed some concerns about over-redacting (taking out sensitive information that is required as evidence to prove the case). In focus groups, we heard lawyers blaming police officers and staff for over-redaction when it was likely that the redaction had been made by CPS operational delivery staff. In some Areas, there was evidence of a risk averse approach, summarised as 'if in doubt, take it out'. There was also a lack of understanding among some legal staff that the unredacted copies of material would still be available to them in the prosecutor bundle.

1.94. Inspectors found that, in cases where the lawyer had less input (overnight remand cases and straightforward guilty plea cases), the roles and responsibilities for checking shared case material were clearer; here, the responsibility falls to operational delivery staff to check and redact before dispatch.

1.95. For cases requiring a lawyer review (not guilty bail cases and cases destined for the Crown Court), the roles were less clear to those we interviewed. In the majority of Areas, lawyers were unable to articulate the role of operational delivery staff in relation to checking documents before the lawyers received

them, or who would be responsible if a bundle containing sensitive material were dispatched.

1.96. Areas would benefit from a clearly defined process identifying roles and responsibilities in relation to redaction itself and to logging cases where redaction is necessary. It would also be helpful if all staff had a clear understanding of the whole process, not just their individual roles. This would also reduce the growing concern that operational delivery staff are being asked, in effect, to make legal decisions on cases given the pressurised time limits they often face.

Recommendation
A consistent process for logging redactions and security breaches should be defined and implemented in all Areas to ensure the consistency and accuracy of data.

Retention and destruction

1.97. Inspectors found evidence of a general understanding, across all Areas and most roles, that there was a retention and destruction policy, with destruction dates recorded on the CPS's case management system. The principles of GDPR were being followed and it was clear that systems had in many ways automated the process, which aided Areas greatly.

1.98. Inspectors in Area visits found some awareness that sensitive material other than case material should be checked; reference was made to The Big Tidy Up, to be launched shortly, and to reminders to staff to destroy data held in personal folders in accordance with policy.

6. Training

1.99. The Responsible for Information (RFI) training is provided nationally in the form of e-learning, which is renewed annually and compulsory for all staff. The training is civil service wide and not specific to the Crown Prosecution Service (CPS). There was no evidence of any other nationwide CPS-specific training on information management.

1.100. The CPS launched a new data protection training package on 1 July 2020, which replaced the RFI and is compulsory for all staff and new starters. Some who had completed the new course felt that, although it was an improvement on the RFI, it still did not address CPS-specific issues around the handling of case material. Feedback was mixed, but generally more positive than negative.

1.101. At the Area level, an introduction to information management and the General Data Protection Regulation (GDPR) forms part of the induction for new starters. Within the induction training, there is a session that incorporates case studies about security breaches and includes two bespoke videos. Induction packs are created locally, leading to some inconsistency in terms of what training is actually delivered.

1.102. There was some evidence of local training on redaction in Areas, although the details of the training and to whom it was delivered were unclear. Areas would welcome, and benefit from, a national steer in terms of training and guidance material about redaction. Suggestions were made, as set out in chapter 5, about a set of guiding principles and common exceptions to help operational delivery staff deliver their roles effectively and to achieve consistency nationally.

1.103. Almost all staff we interviewed indicated that they would welcome more training on information management. Some felt that an annual e-learning package was insufficient.

Monitoring of training

1.104. The completion of the RFI e-learning is compulsory. All Areas were aware of the need to monitor completion and had a process in place to do so. In the main, this was the responsibility of the Area's Learning & Development Manager. There was no evidence that this data had to be submitted to CPS Headquarters, which would offer some level of assurance.

1.105. The new data protection package is a compulsory module. We were reassured that rates of completion will be included in Area performance packs and monitored at Area Performance Reviews.

1.106. We found that in most Areas, if a member of staff is responsible for a breach then some form of one-on-one meeting takes place between that individual and their manager. They are often instructed to re-do the RFI e-learning course. We found that this process was inconsistently applied across the Areas. Some staff felt that this course of action would not help prevent further breaches.

1.107. We found that there was no consistency of approach across Areas in cases where staff make multiple breaches or errors. This could result in staff being dealt with differently in different Areas. Staff expressed the view that the process for dealing with those responsible for multiple breaches was not clear. Few cited that the performance management policy would be used.

1.108. In our interviews with CPS Headquarters, there was an opinion expressed that if a member of staff is responsible for three breaches (or five for a paralegal officer), then they should be re-trained. In Areas, there was no awareness of this requirement.

1.109. We were concerned, given the potential impact of security breaches, that a CPS member of staff could be responsible for five breaches and not be subject to any appropriate management action, in accordance with the performance management policy. This highlights a cultural issue and a defeated acceptance that security breaches are inevitable.

Support guidance

1.110. All staff we interviewed felt they had sufficient access to support from within their Area. This support was mainly provided by speaking to colleagues or managers about specific cases. Staff at all levels felt that support and engagement with CPS Headquarters was limited.

1.111. There was evidence that all Areas have a process in place for reporting a breach, which has been communicated through team meetings and emails.

1.112. We found that the processes for reporting and recording breaches within Areas were inconsistent. In some Areas, the responsibility for completing the breach form sits with the individual identifying the breach; in others, it is a manager's responsibility. Although inconsistent, we did find evidence of self-reporting, which shows an understanding that a breach must be reported.

Clear training material

1.113. We found no evidence, in any Area, of specific guidance documents on information management and redaction having been shared with staff. Updates and communications were sent to staff in several ways, including emails from managers or weekly communications. The process differed across Areas and was felt to be a reactive response to problems: usually a breach that needed to be rectified.

Recommendations
The Crown Prosecution Service should develop bespoke training modules for operational delivery staff and legal staff in Areas, defining roles and responsibilities in handling casework material and processes around logging redactions and breaches. This training should be mandatory for all Area staff and a record of completion should be retained and returned to Crown Prosecution Service Headquarters. This should also be a mandatory part of induction for staff in all roles.

1.114. Inspectors found limited evidence of Areas sharing performance data about breaches with staff. However, in CPS Wessex, a monthly poster was sent out which included numbers and identified trends. There was evidence to show that this was effective and had staff engaged. This is potential good practice, because it seemed to have the desired effect of raising the profile of the issue within the Area, and all staff we spoke to knew about the priority of getting it right.

Good practice
A monthly poster informed staff about the latest performance figures and any recent policy changes or ‘need to know’ information. Staff were positive about how this raised the profile of information management and allowed them to clearly understand current issues.

1.115. In some Areas, there was evidence that information management was discussed at team meetings, although it appeared that this only happened when there had been an issue, rather than as a regular occurrence. Again, we felt this was reflective of a reactive rather than proactive approach.

1.116. The vast majority of the material available for managers and staff in all Areas focused on the process for reporting a breach and the correct form to use. There was no evidence of specific guidance about what constitutes a breach. This is clearly linked with the question of what should be redacted.

7. Security breaches

Clear process

1.117. When security breaches are discovered within an Area, staff are under a duty to report those breaches to CPS Headquarters within a set time limit, using a specific form.

1.118. There was a general awareness, in all Areas, of the need to report security breaches. However, there was a marked difference in understanding between senior managers and Facilities, Estates and Security Managers (FESMs), who were more familiar with the process, and many operational staff, who were unclear of the mechanics beyond reporting the breach to a line manager. In Areas, it was often the manager who completed the breach form.

1.119. Both legal staff and operational delivery staff were often unaware of what happened after a breach had been reported. We found no evidence to suggest that information and data about security breaches is shared with staff after the breach is reported. In some Areas, this includes those at management level. This is a missed opportunity for learning lessons and providing effective feedback to prevent future breaches.

1.120. There is a process for dealing with incidents and documents received from the police that would cause a security breach if served unredacted. In such cases, if there is enough time before dispatching or serving the material, it should be returned to the police to redact and resubmit. Only where there is not enough time to do this should CPS staff redact and log it.

1.121. Compliance with this process is inconsistent. Many staff, especially legal staff, indicated that they would simply redact material immediately themselves, regardless of timescales, to make sure it was done. Staff understand that they are responsible, but are unclear whether recording and logging instances where police fail to redact sensitive information has an impact, as they see no discernible improvement from the police.

1.122. There is a commonly held belief that police breaches are under-reported, because CPS staff just redact them themselves without logging them. CPS South West indicated that about 10% of cases where the police have not redacted sensitive material before sending it to the CPS are being captured and logged. We could not assess whether this estimate was right, but in our case sample, the majority of errors originated with incorrect information being contained in the material received from the police.

Communication

1.123. Data and information on security breaches is shared with stakeholders at the strategic level.

1.124. The Areas we visited compile details of security breaches and potential security breaches in a log containing the details and circumstances of each breach. This data is shared with the police forces relevant to each CPS Area. There was evidence that it could be discussed at the meetings Areas hold with their local forces.

1.125. We found that the Areas mostly send monthly redaction log reports to the relevant Chief Constable (or other nominated officer), highlighting where they have redacted material that the police should have redacted before submitting it to the CPS. One Area shared its local guidance on redaction with the police. We were not provided with any evidence that sharing data at this level was having a positive impact on the level or extent of the police's failures to redact sensitive information from case material.

1.126. There was no evidence that the data collated on security breaches is shared in a meaningful way, or that it has resulted in improvement. Staff are not informed about themes or trends from the data, or are informed only in very general terms. Some staff expressed the view that understanding themes would help operational staff to be more aware and look out for things which may lead to a security breach.

Recommendations
Performance data around volumes of redactions and security breaches, both locally and nationally, should form part of the Crown Prosecution Service's data pack, to raise awareness amongst all staff and to make sure Areas are accountable for their performance in this aspect of work. This information should form part of the performance data discussed at Area Performance Reviews.

Awareness

1.127. Areas are aware of the security breach protocol. There is a process for reporting and logging breaches. Managers have been provided with guidance on how best to complete the security breach forms. However, there is no consistent approach to ensuring that all breaches are identified and reported.

1.128. Knowledge and awareness about the breach logs varied from Area to Area. In some Areas, staff at all levels were aware that the circumstances of breaches were recorded in a log that was shared with CPS Headquarters and

the police. In others, managers knew about the logs while administrative and legal staff were less sure. In some Areas, only senior managers and the FESM stated that they knew about the logs.

1.129. We found that in some Areas, there are instructions for managers to dip sample material being sent out on the CPS's case management system and look for security breaches. However, we found that in practice, there is limited dip sampling of the material being sent out. In the Areas that do dip sample, this was sporadic in nature. In some Areas, there was no dip sampling at all in place.

1.130. In no Area was there a system of effective quality assurance to make certain that potential breaches are picked up before being sent out, or that actual breaches are identified, reported, and appropriate action taken. When breaches were identified, this was mostly as a result of self-reporting, or took place after they had been identified later in the casework process.

1.131. Managers at all levels rely on staff to accurately check material before it is dispatched and to report breaches when they do occur. Our file examination found that 10% of breaches (10 out of 98) were identified by the CPS and corrected before serving the material, suggesting that many security breaches are not identified or reported.

1.132. In some Areas, managers acknowledged that not all security breaches would be identified. However, some managers, despite acknowledging the lack of assurance, expressed confidence that security breaches were adequately identified and addressed.

Responsibility

1.133. Staff at all levels expressed the view that the vast majority of security breaches were attributable to unauthorised disclosure in material submitted by the police. Conversely, it was also a common observation that in many instances, the police over-redact material and edit out information that is required to prove the case.

1.134. At an Area level, there is a lack of consistency around where the responsibility for redaction lies. In not guilty anticipated plea cases and cases deemed not suitable for summary trial, which are likely to be sent to the Crown Court, it is generally seen as the reviewing lawyer's responsibility to read the case material and provide instructions to operational delivery staff. This includes instructions on redaction.

1.135. However, this does not always happen, and it is sometimes left to operational support staff to decide what redaction is necessary in those cases,

as in police charged guilty anticipated plea cases and some overnight cases, which are not reviewed by a lawyer before the material is served. The concern is that in these cases, redaction will often involve a level of legal knowledge that operational delivery staff cannot be expected to possess or to exercise.

Performance

1.136. There was a significant number of security breaches within our file sample, so whatever action is being taken does not appear to be effective.

1.137. Many staff we interviewed were of the view that the provision of performance data would be beneficial, because it would raise awareness of issues and things to be aware of in the future.

Internal learning

1.138. We found that there was very little consistent sharing and learning. A lot of information is being logged, and a lot of data is being produced, but it is hard to find any link to this being used to drive improvement. There was no evidence of Areas sharing best practice or themes.

Annex A:
Inspection framework

A. Policy and guidance

Does the CPS have a clear policy available and disseminated to all on the management of information?

1. What evidence is there of a clear policy on information management?
2. Is the structure of CPS Headquarters' information management transparent and clear to all staff?
3. How has policy been delivered to local CPS Areas?
4. How is the awareness of policy monitored and maintained?

B. Internal management of casework

Does the CPS have effective controls and measures in place to ensure information shared is secure and appropriately managed?

1. Is there a clear process for the management of shared case material?
2. How does the CPS ensure compliance with the policy? What monitoring is in place both locally and at CPS Headquarters?
3. Are staff aware of their roles and responsibilities in relation to information management in general and specifically case material?
4. How does the CPS ensure security on documents from cradle to grave – what checks are in place?
5. How does the CPS internally ensure the right people have the right access to material and no-one else?
6. Internally, is there a clear and effective process on document retention and destruction?

C. Training

Does the CPS have suitable knowledge and training resources to ensure the organisation understands information management?

1. Does the CPS offer a sufficient training package on information management to all staff?
2. How is it ensured that responsible staff have had appropriate training on information management?
3. Do managers and staff feel they have sufficient support and guidance on information management?
4. Is training and knowledge material clear and readily accessible for all staff?

D. Security breaches

Is the CPS effective in dealing with security breaches and future proofing Information management risk?

1. Is there a clear process for security breaches?
2. How has the management information around security breaches been communicated?
3. Is it clear Areas are aware of and are following security breach protocol?
4. Is it clear where breaches originate and who is responsible?
5. What evidence around security breach performance is there and how is this actioned?
6. What internal learning is in place and applied to reduce the risk of security breaches?

Annex B:
Interview questions

A. Policy and guidance

General

- What do you understand to be the CPS's policy on information management?
- Are you aware of the different teams within the Security Information and Assurance Division (SIAD)?
- Do you ever have any contact with SIAD? How often?

Is the structure of CPS Headquarters' information management transparent and clear to all staff?

- How clear are you about what the national information management team does?
- How would you get in touch?
- Do you know what team to speak to about each issue?
- Potential to list an acronym for a team in SIAD and ask them what it stands for and what they do. The DSU, SIAD, IMT, FESMs, GDPR, FOI, IMAs, ICO, etc.

B. Internal management of casework

General

- Are there any internal controls around who sees what material? How are staff made aware?
- Is there a process for document retention and destruction?
- What do you make of the process? Is it effective?
- How responsible and effective are the police? Should the breach sit with them or the CPS – how do you resolve issues with the police?
- What checks do you undertake as an Area on delivery of the process?

Is there a clear process for the management of shared case material?

- How do Areas ensure that information that comes from the police is secure and shared appropriately?
- What guidance is the Area applying in relation to the management of shared case material? Is this national or local guidance? (details)
- Does the Area return documents that need redacting to the police? What is the process?
- Has the Area provided specific guidance or desk instructions to staff on what details should be redacted?
- Does the Area follow the CPS Headquarters process on providing the data/information on redactions through monthly spreadsheets to the Area Chief Constable (or equivalent)? How long has the Area been following this process for?

How does the CPS ensure compliance with the policy? What monitoring is in place both locally and at CPS Headquarters?

- What are the expectations for police responses to the redacted data spreadsheets, if any? Are there responses? Is there improvement?

Are staff aware of their roles and responsibilities in relation to information management in general and specifically case material?

- How are Area operational staff made aware of their specific roles and responsibilities in managing case material and other material dependent on their role?
- What communication is in place to ensure that staff are aware of their roles and responsibilities, and to keep staff up to date?
- What guidance is in place to ensure that staff are aware of their roles and responsibilities?
- What monitoring is in place to ensure that staff are aware of their roles and responsibilities?

How does the CPS ensure security on documents from cradle to grave – what checks are in place?

- What Area checks are in place on the handling of documents from cradle to grave?
- What Area action has been taken as a result of checks?

How does the CPS internally ensure the right people have the right access to material and no-one else?

- What checks are in place to ensure that only the right people have access to the right material?

Internally, is there a clear and effective process on document retention and destruction?

- What guidance is the Area using? (national and Area based guidance)
- What Area processes are in place?

C. Training

General

- What training has been undertaken in the Area – who delivered it and when?
- What do you think of the training – does more need to be done? Are you confident that you are up to date on all issues around information management?
- Where would you go to find out more about information management training?
- Whose job do you think information management issues sit with? Should it be with the Area Business Manager?

Does the CPS offer a sufficient training package on information management to all staff?

- What information management training has been delivered locally to staff?
- Was the training package designed at local level or is it a national package?
- Who delivered the training? Was it evaluated?
- Do you know where to go to find out more about information management training?

How is it ensured that responsible staff have had appropriate training on information management?

- In Area, is the e-learning redone following a reported breach? If so, is this measured in any way for effectiveness? How is this managed when there are multiple breaches?

Do managers and staff feel they have sufficient support and guidance on information management?

- Would you know who to contact locally with any information management concerns?
- Where would you find any information about information management?
- Are you aware of the GDPR rules and retention policies?
- Are you aware of the local and national process in relation to reporting a breach? Do you know how to access the relevant forms to complete?

Is training and knowledge material clear and readily accessible for all staff?

- If you needed to confirm/clarify a point around information management, how would you normally do this?

D. Security breaches

General

- What constitutes a security breach? Where do they tend to come from?
- How do you get to know about security breaches?
- Security breaches – what is the process as much as you understand it?
- Where would you find any information about security breaches? (Internet, Microsoft Teams, Area Business Manager meetings?)
- How much do information management security breaches in particular impact on your role – day to day life, etc.?

Is there a clear process for security breaches?

- What checks are in place to ensure that material which contains security breaches is not dispatched/sent out?
- What is your role in preventing security breaches?
- What are your responsibilities if you identify a security breach?
- Who do you report a breach to?
- Do you provide feedback on security breaches to the police?

- Would you ever rectify a security breach and not report it, eg a simple redaction?
- Do you have a performance objective around security breaches?

How has the management information around security breaches been communicated?

- How are you kept informed about issues regarding security breaches?
- Are issues around security breaches discussed at team meetings? (if not answered above)

What evidence around security breach performance is there and how is this actioned?

- Are you provided with any data or information about how your team is performing with regards to security breaches?
- Do you know how well your Area is performing in terms of security breaches?
- Do you think that lines of communication are adequate?
- Are you aware what, if any, action is taken when someone is identified as being responsible for a security breach?

What internal learning is in place and applied to reduce the risk of security breaches?

- Have you identified common themes which are leading to security breaches?
- What do you consider the main reasons for security breaches?
- What do you think could be done better to improve performance?

HM Crown Prosecution Service Inspectorate

London Office
7th Floor, Tower
102 Petty France
London SW1H 9GL
Tel. 020 7210 1160

York Office
Foss House, Kings Pool
1–2 Peasholme Green
York, North Yorkshire, YO1 7PX
Tel. 01904 54 5490

This document/publication is also available on our website at
justiceinspectorates.gov.uk/hmcpsi