Forensic Capability Network

Forensic Science Regulator Codes of Practice and Conduct ('the Codes') Issue 6 & 7 Gap Analysis

March 2021

Introduction – This document serves as an informative guide correlating the clauses in the Forensic Science Regulator Codes of Practice and Conduct ('the Codes') Issue 6 & 7 to the previous issue. Issue 7 was published as a correction to Issue 6; issue 6 omitted subsection 23.4 in error and that is now restored on page 74 of the Codes.

Accreditation Requirements – The Forensic Science Regulator has updated several deadlines for accreditation, largely as a response to the COVID-19 pandemic. Full details are available in Table 1: Statement of accreditation requirements within Issue 6 of the Codes. Key updates are summarised below:

Incident scene examination (ISO/IEC 17020) – The previously deferred deadline of October 2020 has been extended to October 2022.
Forensic collision investigations (ISO/IEC 17020) – The October 2021 deadline for at least the lead region to have gained accreditation has been extended to October 2022, with the remaining regions/sites becoming accredited extended to October 2023.
Fire scene examination (ISO/IEC 17020) – Deadline remains set for October 2023. The following interim requirements have been extended:

- Interim requirement 1: The Quality Management System shall be established, the Quality Manual drafted, and quality personnel appointed – extended from April 2021 to October 2021.
- Interim requirement 2: the validation/verification of methods and processes shall be complete, and staff competency evidenced against final procedures – extended from October 2021 to April 2022.

Digital forensics – For scene activities (ISO/IEC 17020), the previously deferred October 2020 deadline has been extended to October 2022.
Evidence recovery during the forensic medical examination of complainants of alleged sexual assault e.g. at Sexual Assault Referral Centres – Interim requirement 1 and 2 have been extended to October 2021 and April 2022 respectively.

Summary – The sixth issue of the Codes became effective on February 16th, 2021 and replaces all previously issued versions. UKAS have eluded that the normal four-month implementation period will apply before this version will be used in assessments. The changes are less numerous than when the previous issue was released and largely relate to data security, which were recommended by National Cyber Security Centre previously published in Regulatory Notice 02/2020.

FSR CoPC Issue 6 Clause No.	Emphasis of Change	Summary of text/extract from FSR CoPC Issue 6	Comments
Preface - Statement of Standards and Accreditation Requirements for all forensic units providing forensic science services	Major	Several accreditation deadlines have been extended, which are summarised above.	There is clarification within the Digital Forensics section around CCTV, body worn video and requirements for network capture and/or analysis and Internet intelligence and investigation (inc. open source intelligence from the internet)
12.1.1 – Subcontracting	Minor	Definition expanded to include 'external services which affect the quality of forensic unit's activities'. 'Security' added and clarification that the original forensic unit remains responsible for the overall quality of the work, *including that of any subcontracted element.*	Expands requirements from sub-contractors to also include external services, which previously may have not been recognised in this section. The addition of 'security' clarifies the original forensic unit is responsible for ensuring security of sub-contractors and providers of external services. Internal procedures may need updating to reflect this.
12.1.2 – Subcontracting	New	Forensic unit shall have a procedure and retain records for: a. Defining, reviewing and approving the forensic unit's requirements for subcontracting and using externally provided services; b. Specifying the requirements of the services to the subcontractor or external provider; and c. Ensuring that subcontractors and providers of external services conform to relevant requirements of these Codes.	Procedures and records now explicitly required for this section. Consider reviewing existing procedures to ensure they align with what is required in this section. This section overlaps with ISO/IEC 17025 Externally provided products and services.
15.1.1 – Control of Non-Conforming Testing	Minor	'Judicial criticism' added to the list of significant instances to consider escalating to the FSR.	Consider a mechanism for how this could be collated. Procedures may need revising to include this requirement.
21.2.32 – The Validation Plan	Replacement text	Particularly where this is a plan for the validation of a new method rather than an adopted method (see 21.2.7), it is accepted additional individuals may be needed to provide the breadth of technical knowledge to evaluate the plan. 65 In such cases these individuals shall be listed and their role in supporting the person responsible for sign-off should be recorded.	These individuals 'shall' be listed. Making this a requirement. Sign-off 'should' be recorded. Making this a recommendation.

FSR CoPC Issue 6 Clause No.	Emphasis of Change	Summary of text/extract from FSR CoPC Issue 6	Comments
23.3.1 – Electronic Information Security	Replacement Text	The forensic unit shall have an information security policy which explains how the unit meets its responsibilities outlined in section 23.1.1. The information security policy shall describe the procedures, based on assessed business and security requirements, for the management of electronic information. The forensic unit shall ensure procedures are subject to regular testing, audit and review.	The requirement to have an information security policy remains, as does the requirement to regularly review and audit. The word 'testing' has been added, thought will need to be given how to evidence testing of procedures. 'Regular' commonly suggests at least annually. The new text also clarifies the policy/procedure shall be 'based on assessed business and security requirements'. Evidence of an assessment of business and security requirements will likely be required to satisfy this clause.
23.3.2 – Electronic Information Security	Replacement text	The forensic unit's information security policy shall have processes for the following.	States the policy 'shall' have processes for the following subsections, making this a requirement.
23.3.3 – Access Control to Electronic Information	Replacement text	The access control procedures shall include the identification, authentication, and authorisation of users. Users shall have defined privileges which limit, as far as practical, access to only the information needed and the key operational services they require to perform their roles.	Procedures 'shall' include identification, authentication and authorisation. All three are requirements and there will likely need to be a documented process for each within access control procedures. Again, 'shall' be granted minimum privileges. Consider defining and documenting minimum privilege requirements for individual roles and then implementing. This will likely need to be done retrospectively for existing staff as well as planned for new staff. Evidence of this being implemented will likely need to be available.
23.3.4 – Access Control to Electronic Information	Replacement text	Access shall be removed when users leave their role or the organisation. Reviews should take place at least every 6 months to ensure access rights are still needed - if access rights are no longer needed, they shall be removed.	Access 'shall' be removed – this is a requirement. Consider building this into leavers process/leavers checklist if available. Reviews 'should' take place at least every 6 months, this is a 'should' statement so best to aim for this to avoid having to justify.
23.3.5 – Access Control to Electronic Information	New	Users with administrative rights shall be authenticated using a second factor where this is technically possible.	Second factor authentication 'shall' be in place where technically possible. Suggest focussing on how to achieve this as it is likely technically possible in most scenarios – smartphone apps, security tokens, biometric factors are options, other options may be available.

FSR CoPC Issue 6 Clause No.	Emphasis of Change	Summary of text/extract from FSR CoPC Issue 6	Comments
23.3.6 – Access Control to Electronic Information	New	Accounts with administrative rights shall only be used to perform administrative duties and shall not be used to access e-mail or the Internet - separate accounts shall be provided for this.	Consider formally documenting this in a suitable policy/procedure and including in any training that is associated to being provided with administrative rights. All staff with administrative rights access to forensic systems need to be aware, consider how to evidence these staff are aware. Could this be included in training records?
23.3.7 – Access Control to Electronic Information	New	Authentication failures should be throttled to 10 attempts in 5 minutes or locked out where this is practically possible as per industry norms. Access control mechanisms shall be protected to prevent unauthorised system-wide access.	‘Should’ be throttled – this is a recommendation, but it is likely that if deviating, expect to be required to provide appropriate justification. Unauthorised system-wide access ‘shall’ be protected – consider how to evidence protection. Consider the use of Microsoft Windows directory service on forensic networks or systems, which allows administrators to manage users, applications, data, and various other aspects of the network.

FSR CoPC Issue 6 Clause No.	Emphasis of Change	Summary of text/extract from FSR CoPC Issue 6	Comments
23.3.8 – The Selection, Use and Management of Passwords	New	Procedures for the selection, use and management of passwords should be formulated to help users to generate better passwords. The procedures shall include the following. a. Users should use machine-generated passwords and have appropriate facilities to store them. b. Password managers for the secure storage of passwords should be used where appropriate. Alternatively, users should adopt the 'three random words' technique for generating suitably complex and memorable passphrases. c. Passwords shall be a minimum of 8 characters and have no maximum length. Regular password expiry should not be enforced. However, users shall change their password when it is known (or suspected) that it has been compromised. d. Users should be educated to not use the same passwords for personal and work accounts. e. Passwords shall not be reused for accounts with administrative rights. f. Users should be prevented from selecting easily guessed or commonly used passwords. g. Password should be protected in transit and at rest using appropriate encryption and hashing techniques. h. All default administrative passwords for applications, network equipment and computers shall be changed, and meet the requirements identified above.	There is a mixture of 'shall' and 'should' in this clause, so care needs to be taken when reading. If deviating from a 'should' clause, expect to be required to provide appropriate justification. In some organisations, complying with these requirements will require liaising with IT department(s) that serve more than just the forensic units and consideration will need to be made to ensure that the forensic units' requirements are met by IT. Consider SLA type agreement to outline requirements to IT departments if necessary so that all parties understand their obligations in order to achieve compliance. As with all clauses, consider how to evidence compliance. Consider the use of Microsoft Windows directory service on forensic networks or systems, which allows administrators to manage the password rules for group and user rights. Single user login with shared known passwords should not be allowed. This potentially enables multiple users to log into a generic account, which lacks any traceability through authentication. Consider the use of machine generated passwords, which is best practice. Most units have a password generator application for use when they produce encrypted materials for sending off-site or with reports to the customer. In everyday laboratory use, machine-generated password software could possibly conflict output/results and additional method validation with forensic workstations be required (especially where they are strictly reduced or locked down in respect of installed software applications). Some flexibility here is provided with the use of a three random words method of providing secure passwords (see NCSC).

FSR CoPC Issue 6 Clause No.	Emphasis of Change	Summary of text/extract from FSR CoPC Issue 6	Comments
23.3.9 – Protection Against Malware	New	With the exception of evidence handling where the detection or removal of malware may have an impact or potential impact on the results of examinations or analysis, the procedures for the protection against malware shall include detection and removal of malware using anti-malware software.	Procedures will likely need updating to add further detail specifically relating to the detection and removal of malware. Consider if freeware provides sufficient protection, enterprise level anti-virus and malware control are likely more aligned to the level of protection required. Consider the practice of removal of malware rather than flattening/wiping and re-installation of a system/image/clone and supported with a risk assessment & treatment plan.
23.3.10 – Protection Against Malware	New	Anti-malware software shall be updated when new definitions become available. Anti-malware updates should be overseen by the forensic unit's change procedures to manage any potential impact to the forensic examination process.	Consideration for a procedure in updating anti-virus/malware file signatures. This is a 'shall' requirement. Some units have segregated networks with no forward-facing internet access, making updates sometimes more difficult. Having the correct control measure in place to support this activity will reduce risks in support of this. In some organisations, complying with these requirements will require liaising with IT department(s) that serve more than just the forensic units and consideration will need to be made to ensure that the forensic units' requirements are met by IT.

FSR CoPC Issue 6 Clause No.	Emphasis of Change	Summary of text/extract from FSR CoPC Issue 6	Comments
23.3.11 – Protection Against Malware	New	Anti-malware software shall be installed on all compatible computers and hardware, unless specified operational requirements dictate otherwise. The forensic unit should implement additional anti-malware procedures such as application/executable allow listing.	This is likely to be a small change to most DF units. Procedures may include instances where anti-virus/malware countermeasures are restricted or disabled temporarily to allow a forensic tool process to complete. Consideration should to given to isolating any computers where this activity takes place from the wider network. This should be the exception rather than the norm, and where possible maintain the protection of the anti-malware software. Again, in some organisations, complying with these requirements will require liaising with IT department(s) where networks and forensic machine are centrally managed. The risk against the wider organisation need to be considered and a risk assessment in place.
23.3.12 – Protection Against Malware	New	The forensic unit shall have, or ensure that its IT provider has, procedures in place to protect from website and email-borne malware, caused by drive-by download and phishing attacks.	Little or no change expected in respect of IT providers. Business systems (email) and network shares are usually managed by the IT provider and any organisation wide policy or procedure should be adhered to in the forensic unit. Often access to social media sites is prohibited from IT systems, unless specifically allowed. Forward facing computers used for Digital Forensics (DF) purposes should be likewise protected, using the same countermeasures employed with the general business systems. This can often limit investigatory activities, which can counter balanced with a procedure and control measures in place and exception recording. Consider isolating such activities to stand alone computers/laptops used specifically for this purpose and the recording of access to potentially harmful websites, and/or social media used during investigation.

FSR CoPC Issue 6 Clause No.	Emphasis of Change	Summary of text/extract from FSR CoPC Issue 6	Comments
23.3.13 – Protection Against Malware	New	The forensic unit shall access the Internet via a proxy service which blocks malware. The forensic unit shall have procedures for filtering or blocking phishing Emails or messages, before they reach users.	This will most likely be a significant change for some units and require additional resources with equipment (proxy server) and the management of it. Most organisations have such a service running on the wider business system and good practice established there could be mirrored with forensic computers. IT providers will have the experience, skills and knowledge in the administration of such systems.
23.3.14 – Protection Against Malware	New	The forensic unit shall have procedures to update (patch) software and firmware in a timely manner overseen by the forensic unit's change procedures to manage any potential impact to the forensic examination process.	IT providers usually have procedures for patching business systems. This may be less frequent than the requirements of a DF unit, where computers, systems, firmware and software require more regular patching.
23.3.15 – Protection Against Malware	New	Software and firmware that is no longer supported by vendors, should be replaced unless there is a technical or CJS justification for its continued use recorded in the procedure. 'Critical' and 'High' severity patches for Internet-enabled systems shall be installed as soon as is feasibly possible. Where this is not possible, then other mitigations (such as physical or logical separation) shall be applied.	Antivirus or anti-malware products no longer supported by the supplier/vendor will not provide any continued protection and malware signature file updates will ultimately cease to be provided or be reliable. There will be little or no reasonable justification for continued use, unless the application is a hardware product such as a next generation firewall or high-end router with such AV capabilities built in, and the product becomes no longer supported, and there is nothing else immediately available to replace the infrastructure; however, this is highly unlikely. Patching of operating systems through updates is important and consideration for implementing them shall be done expeditiously, subject to testing to ensure no conflicts against existing operation. Consideration should be given to testing patch updates singularly or in a sandbox environment and review before a wider install against many computers.

FSR CoPC Issue 6 Clause No.	Emphasis of Change	Summary of text/extract from FSR CoPC Issue 6	Comments
23.3.16 – Protection Against Malware	New	All removable storage media shall be scanned using anti-malware software before use.	Consideration to a documented technical procedure for the use of removable media (USB/CD/DVD/eMMC) and using a stand-alone computer that is running enterprise level anti-virus/malware protection to 'sheep dip' before introduction to forensic examination procedures. A risk assessment should be in place for this process, with the examination of cyber related crime and media obtained from computer-based CCTV systems regarded as high risk.
23.3.17 – Protection Against Malware	New	The forensic unit should securely configure computers by following the End User Device security principles.	End user device is a collective term to describe smartphones, laptops and tablets that connect to an organisation's network. The NCSC provides excellent advice in respect of security and this includes 12 principles, such as application whitelisting, auditing, and logging should any problems occur. Use of full or partial encryption with smartphones (use of Knox or equivalent), full disk encryption with computers and in particular laptops. Use of strong passwords, use of VPN, data at rest protection and policies like time to lock screen lock policies such devices. Biometric access and authentication. Enterprise services only accessible through authentication. Secure boot that will not allow any boot process access (use of BIOS/UEFI passwords) Consider the creation of a documented plan to respond to and understand the impact of security incidents. This should be supported by appropriate functionality within the devices and your organisation. In the case of a lost device, this might entail sending a wipe command to the device and revoking credentials.

FSR CoPC Issue 6 Clause No.	Emphasis of Change	Summary of text/extract from FSR CoPC Issue 6	Comments
23.3.18 – Protection Against Malware	New	The forensic unit shall have access to offline backups of electronic information so that it can recover from a ransomware attack.	Consider full OS or 'gold system' build backups for mission critical computers and ensuring these are stored remotely offline and off-site (rather than on a network server). Best practice to store this on alternative media such as LTO tape drive/removable NAS, etc and store securely. Other important archive/backup of evidential data shall also be stored offline (from the forensic systems) to prevent infection across networks from malware. Access should be within reasonable timeframes in which to recover from any malware attack.
23.3.19 – Management of Removable Storage Media	New	The management of removable storage media procedures shall include its issue and use.	Consider including removable media in any equipment register and asset numbering, track its issue and use. A procedure should include instruction on acceptable use of removable devices, for example enforcement in the use of encrypted volumes.
23.3.20 – Management of Removable Storage Media	New	Removable storage media shall only be issued to users whose role requires it. Only the interfaces necessary for the use of removable storage media should be enabled on computers.	Again, consider including removable media in any equipment register and asset numbering, track its issue and use. A risk evaluation and inclusion on a register for allocated staff.

FSR CoPC Issue 6 Clause No.	Emphasis of Change	Summary of text/extract from FSR CoPC Issue 6	Comments
23.3.21 – Management of Removable Storage Media	New	Personal removable storage media shall not be used for the transfer of electronic information - only officially issued removeable storage media shall be used which: a. Shall be physically secured when not in use; b. Should not be used to take data offsite unless its contents are secured using appropriate encryption techniques; and c. Should be subject to accounting with the aim of tracking use and managing loss.	Include removable media in any equipment register and asset numbering, track its issue and use. A policy should be in place to provide instruction and support in the use of removable media, with a technical procedure or work instruction in safe usage. Consider the use of Windows system/registry function or edit to restrict/allow the installation and usage of specifically approved USB devices. Consider the use of software or hardware encryption (with use of strong passwords as described above) being available with devices and a policy to ensure its use. Whilst this clause requires encryption to be used on removable media taken off-site, consider risks of use on-site and whether the requirement for encryption should be global if there are no technical reasons to the contrary. A policy should include instruction on what is not allowed to be used on systems. For example, home/personal use removable devices, lost/found devices for attribution discovery, and items submitted to CCTV units purposing to contain video footage from systems of unknown province and private usage.
23.3.22 – The Segregation of Forensic Networks	New	The forensic unit shall have procedures for the segregation of systems used for forensic science work from other networks. Systems and data that do not need to communicate or interact with each other should be separated into different network segments, and only allow users to access a segment where needed. Segregation can be achieved physically or 'logically'. Logical separation can include access control lists, network and computer virtualisation, firewalling, and network encryption such as Internet Protocol Security (IPSec).	Most units have segregated networks for use in DF; however, many are now incorporated onto the wider business systems and managed through the IT provider with separation through virtual networks or physical (with managed firewalls and monitoring systems in place). Group and user policy restrictions should be employed with only administrative type privileges given to those who require it. A risk assessment should support this policy. Consideration should be given to restricting and governing which staff can delete files & folders from evidence repositories.

FSR CoPC Issue 6 Clause No.	Emphasis of Change	Summary of text/extract from FSR CoPC Issue 6	Comments
23.3.23 – Backups, Recovery and Business Continuity	New	The forensic unit shall have procedures for business continuity with an incident management plan including backup and retrieval of data, to recover from incidents such as ransomware, theft or hardware failure, whilst ensuring the business can continue to function.	Procedures should be well documented, technically detailed to ensure continuation of the service subject to staff and dept changes, and be periodically recovery tested. Consider backups of the operating systems of mission critical forensic workstations or servers so that recovery to a functioning system is possible in reasonable timescales. Virtualisation of some systems may provide a more cost-effective solution and provide swifter recovery in the event of a disaster.
23.3.24 – Backups, Recovery and Business Continuity	New	Where digital data is the evidence, the procedure should be risk-based, balancing consideration of the time between creation of the extracted material, retention of the evidential device and any identified off-site back-up requirement.	A risk assessment should be in place with considerations that support the decision-making process Consider updating procedures to additionally create a master backup copy of evidential material at the time of capture and preservation. Some software tools allow the creation of two sets of identical E01 files, saved to separate locations (which may reduce the time and effort), or use of sync software to replicate data across a network to a backup repository. This may be a significant change for some units and require additional resources This should be risk-based, balance of the time between creation of the extracted material, retention of the evidential device and any identified off-site back-up requirement.
23.3.25 – Backups, Recovery and Business Continuity	New	The forensic unit shall identify what electronic information is essential to keeping operations running and make regular backup copies, or where that infrastructure is provided by the larger organisation (e.g. police force) seek assurance the backup is adequate.	Consider documenting what information is required for backing-up and inclusion in a risk assessment to support the decision-making process. IT providers will require evidence records/logs of testing/regular use of the restoration function and any backup process in place. Essential data may be technical records, case submission information, reports and findings.

FSR CoPC Issue 6 Clause No.	Emphasis of Change	Summary of text/extract from FSR CoPC Issue 6	Comments
23.3.26 – Backups, Recovery and Business Continuity	New	The forensic unit shall identify its critical systems and have redundancy arrangements in place. The forensic unit shall test that backups are working to ensure it can restore the electronic information from them in the event of an incident. Offline backups shall be created and stored for as long as necessary to meet the requirements of the Criminal Justice System.	IT providers will require evidence records/logs of testing/regular use of the restoration function and any backup process in place. Backups conducted by forensics staff will require a documented procedure in place and assurance that it can be restored in the event of an incident. This is likely to require additional resources and processes to be in place.
23.3.27 – Backups, Recovery and Business Continuity	New	Offline backups should be stored at a separate and secure location. The forensic unit may use appropriate cloud services for this back-up of electronic information; 'offline' here means digitally disconnected when not in use and designed to remain unaffected should any incident impact the live environment.	Any solution should be supported with a risk assessment and detailed mitigation if a cloud-based solution adopted. A separate location means a separate building not merely a separate room. Exceptions to this requirement will be rare but may include forensic units with specific high-security requirements. Back-ups also need to be secured from potential malware or ransomware attacks so offline backup is expected. Some flexibility is incorporated with the additional wording at clause 23.3.20 - Where digital data is the evidence, the procedure should be risk-based, balancing consideration of the time between creation of the extracted material, retention of the evidential device and any identified off-site back-up requirement.

FSR CoPC Issue 6 Clause No.	Emphasis of Change	Summary of text/extract from FSR CoPC Issue 6	Comments
23.3.28 – Backups, Recovery and Business Continuity	New	The forensic unit shall have an incident management plan which helps staff identify, respond to and recover from incidents as well as continue to run the business. The incident management plan should include a communication strategy, roles and responsibilities of staff and third parties such as service providers and authorities, as well as contact details for those involved.	Some units have a Business Continuity Plan (BCP) and this requirement should link and support this. Slight changing of wording within the BCP to include incident elements rather than just continuity. Examples of incidents could be a security breach (physical) or data incident such as a ransomware attack. Include a communication strategy where there are requirements to make notifications of incidents to associated bodies, such as the ICO, FSR, UKAS and FCN. A risk assessment detailing these possible notifications with potential impact & significance should be included (i.e. High risk to organisational reputation).
23.3.29 – Backups, Recovery and Business Continuity	New	The forensic unit shall periodically test the incident management plan to ensure that its electronic information and critical systems can be recovered in the event of an incident, whilst ensuring that the business can continue to operate. Revisions to the incident management plan should include lessons learnt to ensure the same event cannot occur in the same way again.	Again, consider inclusion of incident management in the BCP.
23.3.30 – Network Security and Mobile Working	New	The network security and mobile working procedures shall include the management of the network perimeter by using firewalls to create a 'buffer zone' between the Internet (and other untrusted networks) and the networks used by the business.	Consider a detailed network map with a DMZ included with the configuration positioning of firewalls, databases, data stores and servers.
23.3.31 – Network Security and Mobile Working	New	The forensic unit shall have procedures to protect its internal networks by ensuring there is no direct routing between internal and external networks (especially the Internet). The forensic unit shall have procedures for securing wireless access to its networks. All wireless access points shall be secured using Wi-Fi Protected Access2 (WPA2) or WPA3, and only allow known devices to connect to corporate Wi-Fi services.	The use of WiFi networks is a risk and should be included in any risk assessment for the laboratory areas. If possible, use should be avoided; however, there may be operational and business requirements to allow such a network. A documented procedure and policy on its use is recommended. Consider additional security measures such as known MAC enabled access only as well as WPA2/3 protocols.

FSR CoPC Issue 6 Clause No.	Emphasis of Change	Summary of text/extract from FSR CoPC Issue 6	Comments
23.3.32 – Network Security and Mobile Working	New	Where mobile working is required, the forensic unit shall have procedures for ensuring that connections are identified, authenticated (preferably using multiple factors) and authorised. All electronic information which transits the Internet (and other untrusted networks) shall be protected from eavesdropping and alteration using appropriate encryption such as IPSec and Transport Layer Security (TLS).	Consider the recording and storage of firewall logs for event tracing should an incident require investigation. Where access to the internet is required for investigatory purposes also consider the use of VPNs (Virtual Private Networks) by default. This may require additional resources such as VPN accounts or software (Note: VPN sometimes included in enterprise level anti-virus end point security solutions). Any email correspondence should be encrypted through use of protocols such as TLS. This is often a settings option with most client or webmail applications (for example Gmail always uses TLS by default). Consider use of Terms of Reference (TOR) for web research & browsing where possible, making sure to follow good practice guidance with this (i.e. no full screen browser use). Consider the training and competence of staff engaging in online activity and implications of leaving digital traces online (i.e. browser fingerprinting, IP logging). Staff should be discouraged from using identifiable Bluetooth device account names or inappropriate SSID identification as this may compromise the organisational reputation.

FSR CoPC Issue 6 Clause No.	Emphasis of Change	Summary of text/extract from FSR CoPC Issue 6	Comments
23.3.33 – Network Security and Mobile Working	New	All mobile devices shall only have the necessary applications and electronic information to fulfil the business activity that is being delivered outside the normal office environment. If the mobile device supports it, data shall be encrypted at rest. The forensic unit should ensure there are adequate procedures for monitoring network traffic for unusual incoming and outgoing activity that could be indicative of an attack. The forensic unit should have procedures for testing the security of its networks.	Consider the use of PEN testing services to independently assess vulnerabilities to networks and identify risks. This may include a review of system patches and their status. Mobile devices disk drive/data stores should be encrypted by default. If BitLocker is used, ensure that Windows 10 Pro is installed as this supports this encryption. BitLocker creates a secure environment for data at rest. Good practice is to deploy some form of Intrusion Detection System (IDS) on a forward-facing network. Some units use a separate broadband account for research, development and some investigation purposes. This should be separate from the wider organisation and exclusive to the teams use. Where possible, use of broadband services for this purpose should be covert or obfuscated from identification to the organisation. A combination of VPN and obfuscated accounts could be a solution rather than a fully covert account.
23.3.34 – Use of Cloud-Based Services	New	The process for the use of cloud-based services shall include procedures to: a. determine the business need and end-user requirements; b. identify what data and information will be transported, stored and processed, and understand the associated risks; c. evaluate the security of the offering; and d. understand the residual risks and how these will be managed.	Again, consider a risk assessment of any cloud-based solutions or activity.
23.3.35 – Use of Cloud-Based Services	New	The forensic unit should use cloud providers which meet the NCSC's cloud security principles. The storage and processing of evidential data and information using cloud-based services should only be performed from data centres physically located in the UK. The forensic unit should periodically review whether the cloud-based services still meet their business and security needs.	These principles can be found on the NCSC website. These broadly align to good practices cited within the above clauses.

FSR CoPC Issue 6 Clause No.	Emphasis of Change	Summary of text/extract from FSR CoPC Issue 6	Comments
23.3.36 – Security Monitoring and Situational Awareness	New	The security monitoring and situational awareness procedures shall include the generation, capture, retention, storage and analysis of logs from its computers and network equipment. The forensic unit's security monitoring procedures shall: a. provide visibility of communication between their network and other networks (i.e. the Internet or 3rd party suppliers); b. capture authentication and access attempts; and c. provide asset and configuration information. All logs shall be stored securely so they are safe from tampering and unauthorised access. All logs should be stored for a minimum of 6 months so that they can be used to support incident management.	Consider a procedure for capturing event system and security logs for mission critical computers and computers used in forensic processes, including servers. This will potentially require additional commitment in resources and management of information. A retention policy should be in place in support of the procedure. Logging in this manner can generate vast amounts of data and a server or NAS based solution may be required as a store. In addition, such data may be part of the backup and archiving procedure. Firewall and IDS logs shall be included, and this may also form part of a routine backup. System builds and asset records are required to be recorded and stored securely. Most DFU's have asset registers that are well managed, and this clause is not to replace existing equipment procedures but rather to include the not so obvious, but critical, equipment in the register (for example temporary NAS or RAIIDs).
28.3.1 – Types of Report in the CJS	Minor	In relation to SFR1 'it does require a statement of whether the forensic unit is accredited.' has been replaced with 'It does however require a statement of whether the results are from a method which requires accreditation and if so, if the method is within the forensic unit's schedule of accreditation.' There is also clarification that SFR2 is intended to be presented in evidence unless a full-evaluative statement is required instead.	Adds clarity to the level of detail required in SFR1 regarding accreditation
28.6.2 – Defence Examinations	Replacement text	The forensic unit appointed by the prosecution shall have defined policies and procedures to facilitate access by defence examiners to carry out a review of work already completed by the forensic unit, which is deemed by the prosecutor or court to be relevant, in the case.	The forensic unit appointed by the prosecution 'shall' have defined policies and procedures. Making this a requirement

FSR CoPC Issue 6 Clause No.	Emphasis of Change	Summary of text/extract from FSR CoPC Issue 6	Comments
28.6.4 – Defence Examinations	Replacement text	The policies and procedures shall ensure the security and integrity of the exhibits and records requested for review, but must also ensure the confidentiality of other work in progress or previously undertaken by the forensic unit instructed by the prosecution, to which access has not been granted.	The policies and procedures 'shall'. Making this a requirement.
28.6.10 - Defence Examinations	Minor	'recorded' and 'any conditions that apply to handling and retention are made in writing (e.g. from the court, prosecution, customer).' have been added to this section.	