Minutes – Minutes – Minutes – Minutes – Minutes – Minutes – Minutes – Minutes

Forensic Science Regulator

Digital Forensics Specialist Group (DFSG) meeting

Note of the meeting held on 15th May 2026 online via MS Teams

1. Welcome, Actions and Minutes

1.1.1 The Chair welcomed the group and thanked members for attending.

1.2 Previous DFSG Minutes

1.2.1 The Chair invited comments on the minutes from the DFSG meeting held on 02/02/2026, which had been circulated in advance. No corrections or comments were raised, and OFSR will publish the finalised 02/02/2026 minutes.

1.3 DFSG Action Log

1.3.1 The actions from the previous meeting were reviewed, with all items confirmed as completed.

2. Subgroup Updates

OFSR provided an update on both subgroups which sit under DFSG.

2.1 DIG 100 Subgroup (DIG100SG)

2.1.1 Discussions have focused on preparations for the Code of Practice (Code) version 3, including digital scene activity, vehicle system forensics, and broader compliance considerations. The group has also reviewed elements of DIG 102.

2.2 DIG Audio Working Group (DIGAudioWG)

2.2.1 A newly formed task and finish working group to review and update the obsolete Speech and Audio appendix (FSR-C-134) and to review the sub-activities within the following FSA's:

a. DIG 400: Audio acquisition, conversion and processing and;
b. DIG 401: Speech and Audio analysis

2.2.2 The group is using the obsolete appendix FSR-C-134 "Speech and Audio Forensic Services" as a foundation to create a stand-alone Specific Requirement for Audio and Speech. The group includes representatives from policing, academia, and the commercial sector.

3. Artificial Intelligence (AI)

3.1.1 The group discussed emerging considerations relating to the use of Artificial Intelligence (AI) within digital forensics and the potential implications for regulation. It was noted that the Regulator may secure short-term funding to for a project to focus specifically on AI in the context of the Code.

3.1.2 Group members acknowledged that AI-enabled functionality is already present in some tools and is likely to become more widespread. While there is currently limited visibility of how digital forensic units are deploying these capabilities, it was agreed that this represents an area requiring early consideration to ensure appropriate governance.

3.1.3 The discussion focused on the need to understand how AI tools can be validated, tested, and used appropriately, including the development of suitable guardrails and expectations for their use. Concerns were raised regarding the reliability of some AI systems, particularly large language models (LLMs), and the potential risks of relying on outputs that may not be fully explainable or consistent.

3.1.4 Members discussed the distinction between different uses of AI, noting that more structured applications (e.g. classification tasks) may be more straightforward to assess than broader question-answering or interpretive uses, which present greater complexity. Concerns were raised about the

potential for bias, inconsistency, and over-reliance on AI outputs in investigative decision-making.

3.1.5 The importance of transparency and auditability was highlighted, with members noting that it will be critical to document how AI tools are used, including inputs, outputs, and any subsequent actions, to support scrutiny and disclosure requirements.

3.1.6 It was emphasised that clear audit trails (including but not limited to prompts, outputs, and decision-making steps) will be essential to support disclosure and evidential scrutiny.

3.1.7 It was also noted that there are existing work and research in this area, and opportunities to engage with other teams and initiatives to avoid duplication and ensure alignment with broader developments in AI governance.

4. Code Version 3 Update

4.1.1 OFSR detailed that the intention for the Code version 3 is to include all FSA's detailed within the Code. OFSR confirmed that DIG 101, DIG 102 and DIG 401 are expected to be brought into scope. While there is a clearer direction for DIG 401, the approach for DIG 101 and DIG 102 remains under development and has yet to be finalised.

4.1.2 The group noted that DIG100 currently operates as a device-agnostic FSA, covering data from any source. As part of ongoing work, consideration is being given to the potential introduction of a new vehicle systems and telematics FSA.

Vehicles, Drones and Legislative Considerations

4.1.3 The group discussed the potential scope of a vehicle systems and telematics FSA, including whether this should include drones.

4.1.4 It was highlighted that while there is limited accreditation for the extraction of data from drones, there is currently no accreditation for more complex analytical activities, such as determining payload or origin. This creates a gap which would need to be addressed if drones were incorporated into the Code.

4.1.5 The discussion also identified legislative challenges, particularly where existing exclusions (e.g. Investigatory Powers Act and Overseas Production Orders) conflict with areas such as telematics and call data records. It was agreed that these exclusions would need to be reviewed and potentially revised to enable proper inclusion within the Code.

DIG 101 and DIG 102

4.1.6 The group discussed the current positioning of DIG 101 (Analysis of communications network data) and DIG 102 (Digital network capture and analysis). DIG 102 was recognised as covering a broad range of network forensic activities, particularly those involving systems that cannot be seized. It was noted that this presents challenges for applying existing accreditation standards, particularly where extraction requires support from system administrators at scene.

4.1.7 Members highlighted the complexity of network forensics, noting the wide variation in systems, logs and required expertise. Concerns were also raised regarding potential overlap with intercept-type activity, and the need to ensure that the Code does not unintentionally include activities outside the intended forensic scope.

DIG 300, DIG 301 and Emerging FSA's

4.1.8 The group noted that there are unlikely to be significant changes to DIG 300 (Recovery and processing of footage from closed-circuit television (CCTV)/video surveillance systems (VSS)); however, DIG 301(Specialist video multimedia, recovery, processing and analysis) may be subject to restructuring. In particular, there is an intention to split out analytical activity from extraction activity, which may result in the creation of additional FSAs. However, this restructuring has not yet confirmed and is subject to change.

4.1.9 Facial Recognition was discussed, it is currently excluded from the Code, but the Regulator has indicated a desire to consider reintroducing it across all forms, potentially including live, retrospective, and officer-initiated use. It was suggested that if live facial recognition were to be included, it may require a separate FSA due to its distinct operational characteristics.

Framework Approach, Scenes and Kiosks

4.1.10 The group discussed the broader challenge of achieving accreditation across all areas of DIG 100, particularly for scene activity.

4.1.11 Kiosk use was discussed in relation to the activity:

a. Being widely used but there is a lack of consistent standards
b. The existing dispensation has not been widely achieved
c. There is a need for defined governance controls and clearer expectations within the activity.

It was suggested that a framework approach could be applied to both kiosks and scene activity, providing a structured route towards accreditation while ensuring risks are managed in the short term.

5. DFSG Workplan

5.1 Data Security

5.1.1 The group discussed the current data security section within the Code (Section 26 Data Security), noting that it sits within the main body rather than the digital specific requirements. It was acknowledged that this section was originally drafted several years ago.

5.1.2 Members agreed that the existing content is now outdated and does not reflect current ways of working within digital forensics. In particular, this section does not adequately address developments such as cloud-based systems, software as a service (SaaS), and platforms which require continuous connectivity. It was also noted that the original drafting assumed the feasibility of approaches such as air-gapping, which are no longer realistic for many organisations.

5.1.3 The group recognised that the requirements do not scale well across different organisations, particularly where digital forensic units are managing very large volumes of data. Concerns were raised regarding the significant practical and financial challenges associated with meeting some of the

requirements, particularly in relation to data storage and backup arrangements.

5.1.4 It was noted that data security requirements have, in some cases, presented barriers to accreditation. The group discussed examples where organisations had delayed accreditation or withdrawn from it, with data security cited as a contributing factor. Members also highlighted previous challenges with unclear or overly rigid wording, which had led to difficulties in implementation.

5.1.5 The need to refresh the data security section was agreed. It was proposed that the National Cyber Security Centre be approached in case they are able to support this work; however, it was also recognised that any update would need to be informed by practical input from the digital forensics community to ensure it reflects operational realities.

Action 1: OFSR to draft a problem statement/ scope for refreshing the data security section of the Code.

Action 2: Engage with relevant teams for support in relation to the Data Security section of the code.

5.2 Triage

5.2.1 The group discussed the current position regarding triage, noting a lack of clarity and consistency in how the term is used across policing. It was acknowledged that “triage” carries a wide range of interpretations, and there is a preference to move towards clearer terminology, such as “screening,” to better describe the activity being undertaken.

5.2.2 It was noted that there are effectively two forms of activity being carried out:

a. Pre-seizure screening at scene and;
b. Post-seizure screening prior to or within digital forensic units.

5.2.3 While these activities fall within scope of the Code, no force currently holds accreditation for scene-based activity.

5.2.4 Members raised concerns regarding the current lack of governance and control in this area. It was also noted that triage tools are being used in some

cases outside of accredited environments, often without consistent standards, training, or maintenance.

5.3 Digital Forensics Specific Requirement

5.3.1 The group discussed the current Digital Forensics Specific Requirement and its role within the Code. It was noted that the document is currently limited in scope and does not provide sufficient detail to support consistent application across digital forensic activities.

5.3.2 Members noted that the current content is particularly limited in its coverage of front-end activity, including scene work and “screening” processes. The majority of the detail applies once material has entered the digital forensic unit, leaving a gap in guidance for earlier stages of handling and examination.

5.3.3 The group discussed the need to expand the specific requirement to better reflect the full lifecycle of digital forensic activity, including areas where there are currently known concerns or inconsistencies in practice.

5.3.4 There was agreement that the specific requirement should be developed further to provide clearer and more practical guidance, particularly in relation to high-risk activities such as kiosks, screening, and scene-based work.

Action 3: OFSR to circulate the current digital forensics specific requirement to DFSG members.

Action 4: DFSG members to provide feedback on gaps / missing content within the Digital Forensics Specific Requirements.

6. Risks and Opportunities – Horizon Scanning

6.1.1 Due to timing, the risks and opportunities standing item was combined with the AOB agenda item.

7. AOB

7.1.1 There was no AOB. The Chair thanked members and closed the meeting.

8. Date of next meeting

8.1.1 The next DFSG meeting is scheduled for 20th July 2026.