



**HEDDLU
GOGLEDD CYMRU
NORTH WALES
POLICE**

Response Date: 26/11/2025

2025/1218 - NWP Forensic Department

In response to your recent request for information regarding;

I am requesting under the FOIA I receive following two pieces of information, both relate to me and my cases:

Both information relates to NWP Forensic Department.

1) Earlier in [REDACTED], I was threatened to be killed by stabbing. Incident is between myself [REDACTED] and [REDACTED]. Part of this investigation, two sources of recordings were provided. This was then passed to for forensic analysis. The only information I have is from the local officer, writing;

**[REDACTED]
Just to let you know that after enhancing the footage you provided, it has been decided that [REDACTED] be summoned to Court for a public order offence (Section 5) . He will receive a summons through the post in the next few days.**

and

**[REDACTED]
The matter was in Court on the [REDACTED] pleaded guilty and received a fine and was made to pay Court costs. I'm surprised you haven't had an update from the Court? Post charge, it is normally the Court that would update you.**

FOIA Request: Please produce the forensic report on this investigation.

2) Between [REDACTED] mentioned that he would be submitting a digital evidence produced in the EML format to a Digital Investigator in your Digital Media Team. He might or not have done this.

FOIA Request: Please produce a literature on how Police accepts digital evidence for a forensic study and if in this case, had [REDACTED] submitted any evidence to the Digital Media Team. If this has been done, please produce the forensic report on this investigation.

In relation to 'please produce a literature on how Police accept digital evidence for a forensic study' - please find attached Digital Forensic Unit Service Level Agreement' which relates to the Digital Forensic Investigation Submission process only.

Harm has also been identified in releasing some of the information contained within this document therefore, Section 31 (1) (a) (b) (c) Law Enforcement is to be considered as part of the Public Interest Test. A Public Interest Test has been carried out to weigh up the reasons for and against

Pencadlys yr Heddlu,
Glan-y-Don, Bae Colwyn LL29 8AW
www.heddlugogleddcymru.police.uk

Police Headquarters,
Glan-y-Don, Colwyn Bay LL29 8AW
www.northwales.police.uk

disclosure of the information requested, to ensure the release is in the interest of the public as a whole and not just the applicant.

Harm in respect of s31(1) Law Enforcement

Policing is an information-led activity, and information assurance (which includes information security) is fundamental to how the Police Service manages the challenges faced.

Whilst not questioning the motives of the applicant, it must be taken into account when considering potential harm that a disclosure under the Freedom of Information Act 2000 is made to the world at large, rather than a private correspondence. Specific details of any digital forensic processes used by the force would be extremely useful to those involved in criminality as it would enable them to create a map of tools and, by extension, providers most used by police Forces.

Providing all details contained within this document could have a huge impact on the effective delivery of operational law enforcement as it would leave companies open to cyberattacks which could have devastating consequences.

Public Interest Test:

Factors favouring Disclosure – data would be of interest to the public, namely give insight into the forensic processes used to solve crimes.

Factors favouring Non-Disclosure - Measures are put in place to protect the community we serve and as evidenced within the harm, to provide a detailed list of digital forensic procedure would allow individuals intent on disrupting law enforcement to target specific companies using the information obtained to maximise the impact.

The public entrust the Police Service to make appropriate decisions regarding their safety and protection and the only way of reducing risk is to be cautious with what is placed into the public domain.

Balance Test

The Police Service is charged with enforcing the law, preventing, and detecting crime and protecting the communities we serve. In order to effectively and robustly carry out those duties, services are utilised which are vital to investigating criminal activity. Weakening the mechanisms used to investigate any type of criminal activity would have a detrimental impact on law enforcement as a whole. Therefore, at this moment in time, it is our opinion that the balance test favours against the disclosure.

Personal Data within the document has also been removed under Section 40 (2).

Therefore, in accordance with the Freedom of Information Act 2000, this letter acts as a Refusal Notice under section 17 (1) of the legislation.

Please note: we have only answered in relation to 'literature on how Police accept digital evidence for a forensic study' by providing the SLA which documents the Digital Forensic Investigation Submission process. This is in no way linked to a particular case and therefore does not consider any other investigative procedures that may/may not have been used.

The remainder of your request is exempt under Section 40 (5)(b)(i):

All requests made under Freedom of Information Act (FOIA) are applicant blind, and a Freedom of Information (FOI) request must be treated as such as a public authority will always view any disclosure as into the public domain. This is because FOI requests are disclosures to the world (not just to the applicant making the request), and the data protection rights of a third party would be breached by disclosure.

The provisions in Section 40 (1) to (4) of the Freedom of Information Act exempt personal data from disclosure and Section 1(1) (a) of the FOIA imposes a duty on a public authority to either confirm or deny if it holds information specified in a request.

However, in relation to a request which constitutes the personal data of individual(s) other than the applicant(s) (i.e. the person making the request), section 40(5)(b)(i), further excludes a public authority from complying with the duty imposed by section 1(1)(a) FOIA if complying with that duty would contravene any of the data protection principles under the Data Protection Act 2018 (DPA).

Therefore, the first element that needs to be met before relying on section 40(5) (b) (i) is that the information requested should, if held, constitute the personal data of a third party (i.e. someone other than the person making the request).

Personal data is defined in the DPA as follows:

"...“Personal data” means any information relating to an identified or identifiable living individual (subject to subsection (14)(c)) [and] “Identifiable living individual” means a living individual who can be identified, directly or indirectly, in particular by reference to— (a)an identifier such as a name, an identification number, location data or an online identifier, or (b)one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.”

As FOI requests are disclosures to the world (not just to the applicant making the request), if North Wales Police were to use exemptions against the information requested (rather rely on the use Section 40 (5)(b)(i)) this would provide the public with information about a certain individual or individuals.

However as Section 40(5) (b) (i) specifically refers to giving confirmation or denial ‘to a member of the public’ it could be argued that giving confirmation or denial to the requestor would not necessarily contravene any Data Protection Principles. Nevertheless, even if we confirmed that we held the information, and then withheld it under another exemption of the Act (e.g. Section 40 (2)) the confirmation alone would disclose personal data of the Data subject/s.

The next element I have considered is whether confirming or denying if the information requested is held, would contravene any of the Data Protection principles.

The first Data Protection principle states: ‘that the processing of personal data for any of the law enforcement purposes must be lawful and fair.’ It is our belief that confirmation or denial that North Wales Police hold the information requested would be unfair to those who may/may not fall into the remit of the request, and therefore contravention of the first data protection principle.

This is because simply confirming whether or not North Wales Police holds the information requested would provide personal information, and to do so would not be fair. If North Wales Police confirmed or denied that we held data surrounding an individual/s this would amount to the disclosure of personal data because we would be telling the world something about that individual/s.

Lastly, in terms of the legitimate interests in disclosure, the information requested would be personal to any individual/s it may or may not concern. Therefore, confirmation as to whether or not any information is in fact held would not be of any benefit to the public.

Therefore, in accordance with section 40(5)(b)(i) of the FOIA 2000, I can neither confirm nor deny that this information is held by North Wales Police. This refusal should not be taken to mean that the information you have requested exists or does not exist.

Consequently, in accordance with the Freedom of Information Act 2000, this letter acts as a Refusal Notice under section 17 (1) of the legislation.

THIS INFORMATION HAS BEEN PROVIDED IN RESPONSE TO A REQUEST
UNDER THE FREEDOM OF INFORMATION ACT 2000, AND IS CORRECT AS AT 25/11/2025



**HEDDLU
GOGLEDD CYMRU
NORTH WALES
POLICE**

DIGITAL FORENSIC UNIT SERVICE LEVEL AGREEMENT

Governance:	Crime Services		
Document Type:	Policy		
Policy Owner:	Scientific Support Manager		
Department:	Digital Forensic Unit		
Policy Writer:	Digital Forensic Unit Manager		
Policy Number:	DFU-SLA-001	Version:	1.3
Effective Date:	24/10/2025		
Recommended Review Date:	12 Months from issue		

POLICY

		CHANGE HISTORY		
Version No	Author	Date	Changes	Ratification
1.0	■	18/10/2022	New SLA format issued	
1.1	■	01/06/2023	Updated for FSR Code Compliance	
1.2	■	01/04/2024	Annual Review, Updated due to UKAS actions 269 and 270/2023.	
1.3	■	24/10/2025	Update to Appendix A & for CPS demand and support.	

■

PURPOSE OF THIS SLA

This Service Level Agreement (SLA) is a contract between the NWP Digital Forensic Unit (DFU), as a service provider (either internally or externally) and the end user. This document will define the level of service their customers will receive and detail the expectations of the DFU when receiving requests and submissions from the service users.

SLA review

The SLA will be subject to a review at 12 months from the date of issue to monitor any improvements to customer focus, service delivery and continuous improvement.

When new changes are required, this document will be circulated by the Quality Team to the Approvers for consultation and agreement. Where there are concerns or comments, please contact the Quality Team (by return of email). If agreement/disagreement to proposed changes is not received back to the Quality Team within 10 working days, it will be assumed that the changes have been agreed and the new version of this document issued.

SERVICE PRIORITY

North Wales Police Scientific Support Unit fully supports the force vision of 'Making North Wales Police the safest place to live, work and visit in the UK', with the following priorities:

- Being visible and engaging with our communities
- Focusing on the basics of fighting, preventing and reducing crime
- Providing an excellent service to victims

Staff within SSU recognise their duty to adhere to both the Codes of Ethics and the Forensic Science Regulators' Code of Practice and Conduct to be fair, impartial and to act with honesty and integrity at all times.

SERVICE DELIVERY

The NWP Digital Forensic Unit is accredited to ISO 17025 (see full list of accredited and non accredited activities under services provided). As such, confidential information may be required to be shared with United Kingdom Accreditation Service (UKAS) and the Forensic Science Regulator (FSR) Confidentiality agreements are in place with UKAS and the FSR.

Details of the current scope of accreditation are available on the UKAS website www.UKAS.com customer number 8231.

The Digital Forensic Unit (DFU):

- Forensically examine digital exhibits for evidence utilising a range of specialised software and hardware.
- Offer advice, guidance and technical assistance in all matters relating to a DFU submission.
- Provide impartial evidence for the identification, defence and prosecution of suspects.
- Make the extracted data available, provide viewing facilities to view extracted data that cannot be shared or accessed via the NWP network and technical support to service users.
- Provide Extraction Reports (e.g. Mobile Device Excel spreadsheets), Technical Reports, Streamline Forensic Reports (SFR) and Section 9 evidential statements (MG11) where necessary to assist the court process.
- Assist court proceedings by providing video/audio evidence in a suitable and presentable format.

- Attend Magistrate and Crown Court criminal trials and hearings; providing expert evidence, so assisting the court and jury by interpreting the examination results in a clear and unambiguous format.
- Seek to continuously improve the service that we provide utilising the in place quality management system.

UNIT DESCRIPTION

The DFU within North Wales Police is based at St Asaph DHQ within the Scientific Support Unit (SSU) building and serves the whole of the North Wales Police force area, providing a crucial service in the investigation of all levels of crime.

The DFU specialises in the forensic capture, processing, analysis and presentation of digital data held on computers, servers, networks, mobile devices, Closed Circuit Television (CCTV) and other digital storage devices. This includes the forensic examination of digital exhibits recovered from or in connection with crime, presenting their findings in an evidential format for criminal prosecutions.

The DFU will also assist with the examination of digital crime scenes and offer support and advice to their customers in the investigation of crime involving digital media. This may include the provision of CCTV data recovery at scene, viewing facilities, devices and technical support to service users.

All DFU staff are vetted to a minimum level of Management Vetting with exception given to the DFU Student Intern being Recruitment Vetting. These details are held centrally on the force Human Resources system who will send out email notifications to each individual 3 months prior to the vetting expiring with the relevant document attached.

The DFU is normally staffed between the hours of 7.00am to 17.00pm Monday to Friday...

ROLES AND RESPONSIBILITIES

The DFU is staffed by designated competent Forensic Investigators, comprising of serving Police Officers and Support Staff. The DFU has Technical Support Staff and dedicated Technical Managers who are responsible for the quality assurance of the service delivered by the DFU.

Role	Description	No of Staff (FTE)
Digital Forensic Unit Manager	Oversees the DFU and represents DFU at a force level.	1
Technical Managers	Responsible for Quality Assurance and staff management.	2.5
Operational Managers	Operational decision making and staff management.	2
Technicians	Capture/Archiving/Management of Digital Evidence.	2
MDE Technicians	Capture of data from Mobile Devices.	6
Forensic Video Analysts (CCTV)	Capture/Processing/Analysis of Digital Evidence.	3
Examiners (HTC)	Capture/Processing/Analysis of Digital Evidence.	11
Administrative Technician	Submissions/Appointments	1
Digital Forensic Unit Intern	Supports Administrative function.	1

SERVICES PROVIDED

The DFU conduct investigations in line with the Standard Operating Procedures (SOP) created for all aspects of their business. Copies of DFU SOPs can be made available to any customer upon request but should not be recirculated without prior authorisation from the DFU. DFU Processes are documented below along with their BS EN ISO/IEC ISO 17025:2017 accreditation status.

Service	Accreditation Status
Data Capture from: Computers and digital storage devices • Hard disk drives • Solid state drives • Memory cards • USB flash drives • Compact discs • Digital versatile discs • Apple Mac Devices...	Accredited methods available
Data Capture from: • Windows Tablets... • Floppy Disk Drives • Drones • Satellite Navigation Devices • Cloud*	Not Accredited
Data Capture from a Mobile Devices, Memory card & SIM card	Not Accredited
Processing of extracted data	Not Accredited
CCTV recovery within laboratory.	Not Accredited
CCTV processing	Not Accredited
CCTV compilations for Court Proceedings only	Not Accredited
Analysis of Data*	Not Accredited
Scene Attendance*	Not Accredited
Data Review Facilities*	Not in Scope
Destruction of digital exhibits	Not in Scope

*These services depend on certain criteria being met.

Turn-around Times / Priority Levels

Forensic investigations within the DFU should be completed within the timescales detailed below. The turnaround times are calculated from receipt and acceptance of the exhibit by the DFU to completion of the examination.

...

Consideration will also be given to the type of exhibits, number of exhibits and their relationship to the investigation when assessing timescales. The submissions should be subject to a risk scoring matrix and all cases will be prioritised on the level of risk, regardless of type.

The automated scoring matrix takes into consideration factors such as whether the case involves a vulnerable victim, whether there is an imminent threat to life, whether evidence is at risk of being lost and whether the case involved child abuse / indecent images. It can also evaluate whether the suspect is in a position of trust and/or has access to children. It will also take into account if the evidence is required to support charge and if the suspect is in custody or on bail.

In addition to the matrix scoring, there are multiple considerations when attempting to predict a turn-around time. This includes the data storage capacity, number of submitted devices, level of examination required, the technical difficulty of the extraction process, such as the presence of encryption, the volume of material extracted for review and extractions from security locked, faulty and/or damaged devices. In the event a case will be delayed due to waiting times for unlock codes or repairs, the case will be set to Pending with the customer, Records Management System (RMS) and LIMA updated. Pending cases are reviewed regularly by the DFU management team.

The following time parameters are therefore provided as a guide for primary devices submitted to the DFU with no unexpected complications and have been devised based on the available resources to the unit at this time.

Device Extraction Requiring Analysis

Level of Risk	Anticipated Turn-Around Time
High	0 to 4 weeks
Medium	4 to 8 weeks
Low	8 to 12 weeks

Mobile Device Extractions & CCTV/Audio/Video

Level of Risk	Anticipated Turn-Around Time
Urgent	24 Hours
High	7 Days
Medium	21 Days (Includes a 24 DVR capture)
Low	42 Days

If the circumstances of a case change following submission into the unit, the DFU reserve the right to change the anticipated turnaround time based on the new circumstances. For example, should a mobile device enter the unit for extraction only, but subsequently requires analysis the turnaround time would be changed to reflect that. To ensure impartiality and fairness to all customers, cases are progressed in the order of the anticipated turnaround date which will have been set upon approval into the unit and following a review of a portal submission manager.

If a customer disagrees with the scoring and turnaround time, the customer should request their supervisor to review the case and make contact with DFU Management directly for consideration. Any changes requested to the original submission by the customer should be documented in writing and added to the LIMA case.

...

Restoration of archive data

Should restoration of data from archive be required, a clear **28 day** period will be necessary to restore the data prior to any further work or reviews being arranged.

Deviation from accredited methods

It is inevitable that occasions will arise when the documented procedure cannot be followed exactly. Situations where such circumstances arise could include the examination of new or unique devices never previously encountered or even homemade devices.

Where the documented procedure cannot be followed, full notes will be recorded demonstrating the steps taken during any examination or analysis and the customer notified.

CUSTOMER RESPONSIBILITY

The Digital Forensic Unit (DFU) regards all the employees of North Wales Police as their customers. They will also assist with requests from other Forces/Agencies as required. All individuals and / or groups will be treated fairly and equally.

Customer Definition

Customers of the DFU can include, but is not limited to:

- Criminal Justice Partners
- Chief Officers
- Local Policing Services (LPS) Senior Management Team
- Crime Services Division (CSD) Senior Management Team
- Operational Support Services (OSS) Senior Management Team
- All Police Officers and Police Community Support Officers (PCSO)
- Other Police Forces
- All staff within the Scientific Support Unit (SSU)

Customer Responsibilities

The agreement to provide this level of service relies on the cooperation of all partners. Customers are asked to recognise that the DFU's performance and efficiency is closely aligned to the prompt and correct submission of exhibits and documentation and that the processes involved in some cases are time consuming.

Submission

All submissions should be completed utilising the agreed submission process. It is the customer's responsibility to read the questions and requirements presented during the submission process and ensure that all questions are answered completely and accurately. Submissions that have not been completed fully or accurately will be declined.

...

Submissions involving factory reset mobile phones will be rejected in most circumstances due to the inability to retrieve data from modern phones. In limited circumstances, some data may be recovered (e.g., in older model phones). It may be possible to recover the reset date on some iPhones which may be relevant to a case. If your case involves a factory reset phone, strong justification will be required in order for the examination to progress.

Should a case be rejected, the rationale for the decision will be endorsed on the case OEL accordingly.

Should an examination no longer be required at any point during the investigation, the customer must inform the DFU at the earliest opportunity to prevent data being extracted unnecessarily, illegally or in breach of the General Data Protection Regulations (GDPR).

In the event of a system failure in the submission process, then the customer will be provided with direction by the DFU on the manual 'paper' submission process.

The DFU operates an electronic submission process via the LIMA portal, which should be completed for all cases. Submissions are prioritised by the LIMA case management system based on the information provided by the submitting officer.

The customer is responsible for ensuring details entered into this system are complete and accurate and that they fully read and comply with the instructions presented to them when completing the process. The contents of the submission ultimately determine the expected turnaround time and Forensic Science Activities to be conducted.

Urgent Submissions

Any case submissions considered 'Urgent', as defined below, should be discussed with the management for the DFU. The case will be assessed and prioritised for completion within agreed time parameters.

- An immediate threat or loss of human life, or for the protection of human life, such that a person's life might be endangered if the examination procedure were delayed.
- An exceptionally urgent operational requirement where the acquisition of data will directly assist the prevention or detection of the commission of a serious crime and/or the making of arrests and the seizure of illicit material, and where that operational opportunity could be lost if the examination procedure is delayed.
- A credible and immediate threat to national security or a time critical and unique opportunity to secure, or prevent the loss of, information of vital importance to national security where that threat might be realised, or that opportunity lost, if the examination procedure were delayed.
- Where a DPNa form has been completed, the case should be treated as urgent.

The turnaround times are calculated from receipt and acceptance of the exhibit by the DFU to completion of the examination.

For urgent cases where RMS tasking is unsuitable or unavailable, the submitting officer is responsible for transferring devices to DFU.

Victim/Witness devices

Victim/Witness devices that require a DPNa form will be processed as urgent (extraction of data within 24 hours of acceptance at DFU) in line with the SLA's. Some devices (for example, computer devices) may take several days to extract however, best efforts will be made to return the device to the owner in a timely manner. The customer will

be kept updated on expected turnaround times. Subsequent processing and analysis will then be conducted as normal.

Victim/Witness devices must be brought to the DFU by prior arrangement with DFU management and a completed DPNa form submitted. In the event victim/witness devices arrive without prior arrangement, the turnaround time may be delayed. It is the responsibility of the submitting officer to return the device to the victim.

Officers are responsible for adhering to the relevant NPCC guidance for victim/witness devices.

Sensitive Investigations

On occasion it may be necessary to deviate from the routine submission process when the investigation is considered sensitive. The reason for the sensitivity may be due to the actual nature of the investigation, or the profile of the person subject to that investigation.

Sensitive Investigations may include investigations conducted by the Welsh Extreme Counter Terrorist Unit (WECTU) or Professional Standards Department (PSD).

The Senior Investigating Officer (SIO) for that investigation will be responsible for liaising with DFU Management to set any enhanced security arrangements and agree the submission process.

Packaging

All exhibits must be appropriately packaged, as the provenance and continuity of the device is essential in ensuring the integrity of the device and the material extracted.

Appropriate packaging should include the device being sealed in self-adhesive tamperproof packaging, which bears a printed unique seal number; or closed in plastic packaging, which is sealed with a tamperproof tag bearing a seal number. N.B. Brown paper or bin bags are not considered appropriate.

An exhibit label should also be attached to or printed on the packaging of the exhibit; this should be completed in full by the seizing officer.

The item description should be worded the same as that on the case submission form.

The label should also be signed and dated by persons involved in transportation of the exhibit to the DFU.

The exhibit should also bear an approved printed seized property label showing the Property Tag Number.

On receipt, the DFU staff member should also check the item description endorsed on the exhibit label accurately reflects the contents of the package.

Whilst regrettable, any failure to follow the above guidance or devices not packaged correctly will be returned to the submitting officer and will result in the potential delay of any examinations.

...

In the event of problems or questions arising, advice and guidance should be sought from the DFU staff.

Damage of Property

In some cases, devices will be subject to interference by digital forensic practitioners to gain access to relevant data. The Investigating Officer should be aware of the possibility that device(s) could be returned in a different state from the point of seizure/submission to NWP. This should be taken into consideration when submitting already broken/faulty devices.

Biohazards / Health & Safety issues

Exhibits containing Biohazards or other Health & Safety Issues will be considered for DFU processes providing that the DFU determine they can be done safely and providing this section of the agreement is adhered to by the customer.

Where an exhibit being submitted to the DFU contains any Biohazards or other health & safety issues (such as chemical contamination, electrical safety issues etc.), it is the responsibility of the person submitting the exhibit to:

1. Ensure that the exhibit can be clearly identified as a biohazard or risk by the packaging that it is in for example ensuring that it is in a biohazard marked bag or has hazard tape attached.
2. Ensure that full details relating to the hazard are documented on the LIMA submission.

Devices Requiring Multiple SSU Services

Where a customer requires multiple services for an exhibit within the SSU they should determine which service to submit to first based on the requirements of the investigation. The decision as to which method should be utilised should be determined on a case by case basis and the DFU along with other services are able to provide advice on a case by case basis prior to submission to detail any risks that may be present whilst providing the requested service.

Unit Attendance

On occasion it may be required for a customer to visit the Digital Forensics Unit. Customers must comply with the visitor process in place at all times during this visit. This includes the requirement for all persons to sign in and out of the unit on every occasion.

SCENE ATTENDANCE

Subject to availability and commitments, the DFU Staff can attend a crime scene to assist in the preservation of data, examination and recovery of digital exhibits. This can include during normal working hours and with prior notification and planning outside the core business hours, when assisting with the execution of search warrants or pre-planned events.

Requests during working hours must be made via the LIMA portal and all requests will be subject of assessment to ensure they are proportionate, and the appropriate assistance is provided.

Out of hours requests for 'urgent' digital forensic examinations or scene attendance must be made via the Force Incident Manager (FIM) and directed to the Cadre DI for approval who would in turn contact a DFU manager.

EXAMINATION STRATEGY

An initial Examination Strategy is determined at the Submission Approval stage. The gatekeeper will establish which Forensic Science Activities (FSA's) are required and assign the case to the correct DFU department. Primary devices will be identified and priority will be given to higher risk cases or devices at risk of losing data.

After the Submission Approval Stage, the practitioner will have LIMA and RMS access to all task-relevant information including the case details, which devices have been approved, requirements of the customer, parameters for data capture, particular data of interest and handling information.

Both LIMA and RMS are fully auditable and only relevant information relating to tasks will be accessed.

The examination strategy will be reviewed by the practitioner prior to commencing casework. If the FSA's to be conducted or timescales for the delivery of the results deviate from the initial assessment, the practitioner will update the customer via RMS Occurrence Enquiry Log (OEL).

Devices handled within the DFU typically follow the below examination sequence:

Data Capture > Processing > Analysis (Conducted either by DFU or OIC) > Reporting of Results

Examination will routinely take place in the DFU Laboratory using equipment listed as available for use on the DFU Asset Register.

If there is a requirement for scene attendance, examination may take place at scene. Updates on scene attendance will be dependent on the specific circumstances.

During examination, any limitations to the scope will be highlighted to the customer on an RMS OEL update or within reporting of results.

SAMPLING STRATEGY

Where it is identified that there are a large amount of potential sub exhibits e.g. multiple optical media disks seized under one reference. Where the total number of individual items exceeds 20, a 20% sampling rate will be utilized.

This process is dependent on the case by case circumstances and potential intelligence factors; in certain instances the sample rate may be amended to meet the requirements of the investigation. Where this process is to take place, it will be discussed with the submitting officer.

REPORTS AND RESULTS

The submitting officer should receive automated updates from the case submission system (LIMA) as the case is being progressed. Where possible, final results will be uploaded to NWP force systems (NICE Investigate/RMS) and the customer notified. Results will be available in the following simplified formats:

- Technical Reports
- Images Reports
- Mobile Device Extraction Reports – Excel Spreadsheet
- Streamline Forensic Reports (SFR)
- Section 9 Evidential Statements (MG11)
- CCTV/Audio/Video Exports – Viewable footage, still images, Edits, Compilations for Court Proceedings.

- RMS OEL update.

All reports (including negative results) issued from the DFU will include declarations regarding accreditation status and status of compliance/non-compliance with the Statutory Forensic Science Regulator's Code of Practice (where required). Risk mitigation tables regarding any non-compliance will also be included (Annex B). The FSA's used will be clearly documented within the issued report.

Data Review

On occasion the review process will fall outside the capability or scope of DFU investigators, as it may require intimate knowledge of the investigation and key persons involved.

On such occasions a discussion on the requirement and viability of such work will take place between the DFU investigator, supervisor and the submitting officer prior to any decisions being made.

NOTE: Mobile phone data extracted from devices will fall into the category above and the request for examination and analysis due to technical requirements should be requested by the submitting officer following an initial review of the extracted data.

The DFU has dedicated viewing stations within the unit where submitting officers can conduct reviews of the extracted data in a controlled and monitored environment. Support and assistance will be provided from the DFU staff on technical matters and guidance provided on extracting material deemed relevant to the investigation. Appointments to utilise the viewing stations can only be considered where the data cannot be reviewed by other means.

It is the responsibility of the submitting officer to attend the DFU within the specified time following the extraction of the data. Due to technical limitations, data will be archived after the given time. At this point the officer will be required to justify any requirement to restore the data for future review, which if agreed will be restored for future review within the specified restoration turnaround time as defined above.

In the event sensitive material needs to be taken from the DFU and used elsewhere, for instance in a suspect interview or at Court, the submitting officer should make this request either in person or electronically; providing details of the reason the device is required and LIMA reference number of the case. Subject to assessment and approval, the DFU staff will provide a DFU 'Viewing Laptop' and the material loaded accordingly.

The deployment of a DFU Viewing Laptop will only be authorised where it meets the strict criteria as defined below:

- For the purpose of allowing reports originating from within the DFU, which are unable to be uploaded to the NWP force systems to be viewed.
- For purposes such as sharing a technical report with CPS, the courts or use in interview.

Due to numerous reasons, including the security of the device and the limited number of laptops available, these viewing laptops are not suitable for the purposes of sharing data for OIC review.

Laptops loaned out for these purposes must not have any data added or removed once taken from the DFU and must be kept secure at all times. The person requesting the laptop is ultimately responsible for keeping this data secure and returning the laptop within the agreed time.

The DFU are not equipped to transfer sensitive data for review on other media types, for example USB Hard Drive/Divisional Viewing Laptops.

CCTV data retrieved and held on the DFU server, which is too large for upload to NICE, can be transferred and encrypted to a USB Hard Drive for review. USB hard drives are available from regional CID offices for this purpose and must be brought by the submitting officer to DFU for data transfer to take place.

RETURNS

The DFU should return all devices to seized property following the extraction of the device data, marked with a blue warning 'For Review' label. Exhibits should not be considered for return to the owner until such time that the case has been finished within the CJS, as the exhibit is deemed to be an offline backup of the exhibit data.

It is the responsibility of the submitting officer to review the results of each exhibit prior to considering the return of any items to the owner.

OUTSOURCING

On rare occasions the DFU may need to outsource work submitted for examination. Where outsourcing is required and available, Senior Management will be contacted to authorise the outsourcing procedure and the customer will receive a notification. The notification will include which service provider has been used, the FSA's to be performed and any timescales provided by the external service provider.

All communications and information relating to the case and any work that may have been undertaken by the DFU should be recorded on LIMA.

MONITORING SERVICE DELIVERY

The DFU procedures are documented and can be viewed on the SSU page of SharePoint. The procedures undertaken within the unit are subject to regular internal and external audits as part of the ISO 17025 accreditation. The DFU management will monitor the DFU service delivery / performance.

Scientific Support Unit Website

The SSU website is available on the intranet and provides useful information, guides and contact details for members of the department and others within the workforce.

Feedback

The Scientific Support Unit will actively seek out feedback from its customers in order to ensure that it remains customer focused. All feedback will be recorded whether positive or negative and actions taken as appropriate in order to effectively deal with the feedback received. A customer feedback form is available on the SSU website.

Customers of DFU are encouraged to complete a customer service questionnaire via a hyperlink on the bottom of all SSU emails.

Dissatisfaction, Complaints and Appeals

The DFU welcomes feedback and customers are encouraged to discuss the service they receive, as this can only progress and improve the service provided.

If a customer is dissatisfied with the service provided, every effort should be made to rectify the situation immediately. If this is not possible, the customer should be referred to the Customer Feedback Form or CS Quality Management Team (QMT) who will raise an action against the dissatisfaction. The action will initiate an investigation by DFU Management who will report back to the CS QMT.

If the complaint/appeal has the potential to lead to a miscarriage of justice, attract adverse public interest or jeopardise our accreditation then the Quality Manager and/or Digital Forensic Unit Manager should be informed as soon as possible. The Quality Manager and/or Digital Forensic Unit Manager will then discuss the issue with the Forensic Science Regulator and United Kingdom Accreditation Service (UKAS). Confidentiality agreements are in place with UKAS and the FSR.

Performance measures and monitoring

Each month the DFU management monitors the following performance measures:

- Quality of submissions to the DFU
- Number of exhibits submitted
- Timelines of investigations
- Staff Competencies

All of the above information is discussed at the management meetings and regular team meetings are held with the DFU Staff to encourage and identify areas for improvement, feedback any positive outcomes and resolve any complaints/appeals.

DECLARATION AND LEGALITIES

- a. In line with all Force policies, the overarching purpose of this document is to directly support the PCC police and crime plan objectives. Overall, the intention of this policy is to provide a safer North Wales.
- b. In the writing of this policy cognisance has been taken of the college of policing code of ethics (2014).
- c. North Wales Police policies will be written in accordance with the approved corporate format. The Scientific Support Unit Service Level Agreements are published on the Force Intranet, allowing access to staff and public, where appropriate, on the pages of the public facing Internet site under the Force publication scheme and Freedom of Information Act 2000.
- d. The following main legal requirements have been identified within this policy:
 - Equality Act 2010
 - Human Rights Act 1998
 - The Welsh Language (Wales) Measure 2011 and the Welsh Language Standards for the Chief Constable
 - Data Protection Act 2018
 - Freedom of Information Act 2000
 - Health and Safety Act 1974
- e. This policy has been written giving due regard to the above legislation and has considered the risk of unfair and/or disproportionate impacts on individuals or groups (actual or perceived) and has done so via an equality impact assessment (EIA).
- f. New legislative requirements or changes in Force structure may necessitate a review of this policy document
- ...