Chapter 11: Transmission of Disclosure Information

11.1 Policy

11.1.1 The policy for transmission of disclosure of information detailed in this chapter relates to the disclosure of information to the accused's legal representative only. Where the accused is unrepresented, the guidance set out in Chapter 23 of this manual should be followed.

11.1.2 In terms of the legislation, the prosecutor may disclose information by any means (Criminal Justice and Licensing (Scotland) Act 2010 s160). However, following full consultation with the Law Society, it has been agreed that the primary method of disclosure will be by use of the secure disclosure website (SDW). This will, where practicable, include any productions capable of being scanned and uploaded on to the website.

11.1.3 COPFS must have regard to its legal obligations and those of solicitors under the Data Protection Act 1998. The use of this technology reduces the security risks surrounding hard copy material going missing or being lost and the use of encryption further protects the integrity of the data. The Deputy Information Commissioner has confirmed that the Crown must ensure that defence agents are registered as data controllers prior to disclosure of any information.

11.1.4 Accordingly, in order to satisfy this requirement, defence agents must sign an undertaking confirming that the firm is registered. The undertaking only requires to be signed prior to the first disclosure of information to a defence firm, and not in advance of disclosure to that firm in every case. Where new firms are created or Solicitors leave firms and become sole practitioners they must sign the undertaking anew. Where a firm fails to provide such an undertaking, or cannot otherwise satisfy the Crown that it is registered as a data controller, then disclosure bundles cannot be issued in any format.

11.1.5 COPFS need not disclose again anything that has already been disclosed to the accused in relation to the same matter (whether because the same matter has been the subject of an earlier petition, indictment, or complaint or otherwise) (Criminal Justice and Licensing (Scotland) Act 2010 section 127). If defence agents are requesting repeated disclosure (as a result of losing or misplacing the disclosure information), then they are failing to comply with the seventh data protection principle. The loss of such data is not a matter which should be taken lightly and it is inappropriate that the COPFS response to the loss of such data be, as a matter of routine, to provide a further copy. COPFS will consider all requests to supply a further copy, providing requests for such, including the reasons as to why repeated disclosure is considered necessary, are made in writing by defence agents.

11.1.6 It is crucial that COPFS maintains a comprehensive audit trail in respect of their disclosure obligations. Defence agents or their representatives must be required to sign a receipt in respect of information disclosed to them. This receipt must be retained with the case papers and available to present to the Court in the event of a dispute. In any case where we are unable to show that disclosure has been made COPFS will not be in a position to refuse a request for repeated disclosure.

11.1.7 The use of the secure disclosure website assists in providing an accurate audit trail and a copy of the publication report created by the electronic system should be printed off and placed within the case papers. This can be referred to in

Court if confirmation is needed that the Crown has complied with their disclosure obligation. Further guidance regarding use of the publication report to confirm disclosure and respond to such challenges in Court can be found in **COC 8 of 2012**.

11.1.8 Whilst all agents undertaking criminal work should have registered for the secure disclosure website there may be occasions when an agent involved in a criminal case has not registered or does not have the capacity to access the secure disclosure website and where that is the case then disclosure should be made via use of a pen drive or by handing over hard copies as deemed appropriate. In these limited circumstances it is vital that all disclosure actions are properly documented and receipted Pen drives must **not** be posted to the defence agent. In all such cases, regardless of forum, the defence must uplift the pen drive from a PF Office. In most cases this will be the office where the case is being prepared, however the solicitor can elect to uplift the pen drive from an office more convenient for them. Such requests should be accommodated unless there are exceptional reasons for not doing so.

11.1.9 Transmission of information to the defence by the secure disclosure website ensures that COPFS is taking all reasonable steps to safeguard sensitive information and thus comply with the seventh data protection principle which obliges the COPFS, as a data controller, to take all appropriate technical and organisational measures against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

11.1.10 The emphasis placed on compliance with the seventh data protection principle is that the procedures adopted by a data controller must be adequate to maintain the highest level of security that is reasonably practicable. Therefore, as long as COPFS can demonstrate that it has adequate procedures in place to prevent against the accidental loss of data (and these procedures have been followed), it will not be found in breach of its data protection obligations should any accidental loss actually occur. The policy set down in this chapter sets out those adequate procedures that COPFS has put in place for disclosing information to defence agents.

11.1.11 Any reference in this chapter to a defence agent also includes any authorised agent acting on behalf of the principal agent.

11.2 Disclosure of Statements and Previous Convictions and Outstanding Charges (PCOCs)

11.2.1 Statements and PCOCs should be disclosed via the secure disclosure website as the COPFS primary method of disclosure.

11.2.2 Once witness statements are available to be disclosed in FOS the first step is to prepare and disclose the List of Witnesses. This should be done by checking which witnesses addresses are discloseable. Any that are not discloseable should be redacted from the list. Thereafter a binder should be created and the list of witnesses should be published on the secure disclosure website.

11.2.3 The second step is to prepare and disclose all witness statements and any previous convictions and outstanding charges (PCOCs) relating to witnesses. This should be done by checking whether the witness statements or PCOCs require to be redacted. Once they are redacted a binder should be created and the witness statements and PCOCs relating to witnesses should be published on the secure disclosure website.

11.2.5 Full guidance outlining the processes for uploading material onto the secure disclosure website is contained in the Case Processing Manual.

11.11 Disclosure of Productions

11.11.1 Productions should be disclosed via the secure disclosure website where possible.

11.11.2 A production record should be added in FOS for each production. Many of these will be done automatically when the Police submit an SPR2 however some may have to be added manually.

11.11.3 Productions should be redacted if required and thereafter scanned in to the system and a binder should be created using Disclosure Manual Client. The binder should be published on the secure disclosure website. This should be done separately for each accused in a case with multiple accused.

11.11.4 Full guidance outlining the processes for uploading material onto the secure disclosure website is contained in the Case Processing Manual

11.3 Subsequent Disclosure of Additional Information in all cases

11.3.1 Where any additional statements or productions require to be disclosed to the defence agents, then the same procedures should be followed.

11.6 Disclosure of Information in Court – High Court Cases

11.6.1 Whenever a case is calling in court, a blank Court Disclosure Minute Sheet should be placed with the court papers for use by the Advocate Depute in court. This should be done by High Court Registry when preparing the papers for Court and should be slotted into the AD's blue folder, next to the standard minute sheets.

11.6.2 Where copies of information are provided to the defence in court, then this should be clearly recorded on the Court Disclosure Minute sheet by the Advocate Depute or the Crown Junior.

11.6.3 Where the defence are given access to any information in court, then this should be clearly recorded on the Court Disclosure Minute sheet.

11.6.4 After court, the Court Disclosure Minute Sheet should be returned to High Court Registry who should then update this information on the electronic copy of the Disclosure Page.

11.7 Disclosure of Information in Court – Sheriff and Jury Cases

11.7.1 Whenever a case is calling in court, a blank Court Disclosure Minute Sheet should be placed with the court papers for use by the Depute in court. This should be done by the appropriate member of solemn administrative staff.

11.7.2 Where copies of information are provided to the defence in court, then this should be clearly recorded on the Court Disclosure Minute sheet.

11.7.3 Where the defence are given access to any information in court, then this should be clearly recorded on the Court Disclosure Minute sheet.

11.7.4 After court, the Court Disclosure Minute Sheet should be returned to solemn administrative staff who should then update this information on the electronic copy of the Disclosure Page. It is the responsibility of the Solemn Administrative Manager to identify the appropriate member of staff to complete this work.

11.8 Disclosure of Information in Court – Summary Cases

11.8.1 Where, due to exceptional circumstances, any additional information is provided to the defence agents in court, this must be clearly minuted in the case papers.

11.9 Disclosure of Information by Access

11.9.1 Where the defence agent is provided access to view information, and are not provided with a copy, e.g. label productions; photographs of indecent images; video tapes of joint interviews with children, a record of this must be kept.

11.9.2 In all solemn cases, this should be carefully recorded on the Disclosure Page of the precognition. This should clearly state the date the information was viewed, the name of the member of staff who supervised the access and precise details of the information accessed by the defence.

11.9.3 In all summary cases, the following information should be recorded in the case papers: the date the information is accessed by the defence agent, the name of the person supervising access and precise details of the actual information accessed.

11.12 Disclosure of Information by E-mail

11.12.1 Ordinary e-mail sent via the Internet is <u>not</u> a secure means of communication and <u>must not</u> be used for the transmission of information regardless of whether the statement fits the criteria necessary to allow electronic disclosure.

11.13 Disclosure of Information by other means

11.13.1 Statements and Criminal History Records should always be disclosed on the secure disclosure website.

11.13.2 Productions should always, where possible, be disclosed on the secure disclosure website. However, where the production is not in a format which is compatible with the secure disclosure website, then the production can be disclosed using a different format, for example on a CD, DVD or encrypted pen drive.

11.13.3 Where productions are disclosed on a different format staff should ensure that the disclosure is properly recorded and that a receipt is available which clearly reflects the items disclosed.

11.15 Defence as Data Controllers of the Information Disclosed

11.15.1 A data controller is defined as *"a person who (either alone or jointly in common with other persons) determines the purposes for which and the manner in*

which any personal data are…processed". Processing is held to include obtaining, recording, holding or using personal data or information. Accordingly, it should be noted, that where defence agents during the course of their business, enter details about identifiable individuals onto a computer, or retain such data as part of a recognised filing system, they must submit a notification to the Information Commissioner's Office, and if they fail to do so, they could be prosecuted. A failure to so register is a breach of the data protection legislation and could expose the defence agents to a fine. The defence agent could also be liable to prosecution under section 17(1) of the Data Protection Act 1998 for processing personal data where there is no entry in respect of them included in the register maintained by the Information Commissioner

11.15.2 As data controllers, defence agents are also bound by the data protection legislation and are required to adhere to the eight principles of data protection, including the seventh principle relating to take adequate steps against accidental loss or destruction of, or damage to, personal data.