**JOINT PRINCIPLES FOR REDACTION**

**This guidance applies equally to both pre and post charge submissions.**

1. **Summary of Key Principles**

We are all responsible for protecting personal and sensitive personal data disclosed in the course of an investigation or prosecution. Personal and sensitive personal data should not be shared between organisations unless for a lawful purpose e.g. it is relevant to an issue in a case or meets the test for disclosure (either common law or under the Criminal Procedure and Investigations Act 1996 (CPIA 1996)).

The unnecessary disclosure of personal data breaches the Data Protection Act 2018 and can have significant consequences including:

* For victims; witnesses or individuals the data relates to by causing them embarrassment; or placing them at risk of intimidation, assault or in the most serious cases death;
* Reducing confidence in the Criminal Justice System;
* Reducing the likelihood that victims and witnesses will report incidents to the Police and co-operate with a prosecution;
* Having a detrimental impact on case outcomes;
* Causing reputational damage to the CPS; Police and the wider Criminal Justice System;
* Having a financial impact on the CPS and Police through fines imposed by the Information Commissioner.

We can protect personal and sensitive data by redacting it from material and information we share.

* The Police are responsible for redacting personal and sensitive personal data from material and information sent to the CPS unless the disclosure of that data is required for a law enforcement purpose. This means the information is needed to enable the CPS to make a charging decision; to support the ongoing review of a case; or to discharge disclosure duties under common law; the CPIA 1996 or the CPIA Code of Practice.
* The CPS is responsible for ensuring:
  + it only handles personal data received from the Police if it is required for a law enforcement purpose.
  + that personal and sensitive personal data is not disclosed to any third party including the Defence and Court unless that disclosure is for a law enforcement purpose.

1. **Introduction**

Redaction is the term used to describe the editing of text or information from material for legal or security reasons. Material includes statements, documentary exhibits, audio and video recordings, digital material, and other sources of information such as crime reports.

Understanding why we need to redact and the legal basis for doing so ensures we process and share material safely and in accordance with our obligations under:

* the Data Protection Act 2018 (DPA); and
* the Criminal Procedure and Investigation Act 1996 (CPIA 1996) / CPIA Code of Practice (CPIA Code).

The DPA is intended to protect and safeguard an individual’s personal and sensitive personal data. It creates a regime (Part 3) that applies to data processing by organisations with a law enforcement function, which includes the Police and CPS. The regime under Part 3 of the DPA is separate from the UK General Data Protection Regulations (UK GDPR).

The CPIA 1996 is intended to ensure an individuals’ right to a fair trial. This is achieved through a fair investigation and disclosure of material to the defence that either undermines the prosecution case or assists the defence case.

Redaction allows the Police and CPS to share and serve:

* Material and information which is either relevant to proving the case or meets the test for disclosure under either common law or CPIA 1996, by redacting personal and sensitive personal data with no relevance to any issues in the case; and,
* Comply with distinct disclosure obligations relating to the handling of **Sensitive Material**  defined in the CPIA 1996.

In summary redaction allows the Police and CPS to share and serve evidence and unused material required to progress investigations and prosecutions whilst also protecting and safeguarding personal and sensitive data. Redaction also allows the CPS and the Police to protect material, other than DPA personal and sensitive personal data, that is sensitive as defined in the CPIA 1996.

1. **Key Definitions and Principles**

A number of principles and definitions from the CPIA 1996; CPIA Code; the DPA and the Attorney General Guidelines on Disclosure 2020 (AGG) highlight how investigators and prosecutors need to be aware of the balance between the right to a fair trial and the right to private and family life (see para 11-13 AGG 2020).

Criminal Investigations should be conducted in accordance with the CPIA Code. Paragraph 3.5 of the CPIA Code requires investigators to pursue all ***reasonable lines of inquiry***, whether these point towards or away from the suspect. Pursing all reasonable lines of inquiry means that the investigation will produce and gather **material** which may be **relevant material.**

***Material*** *is defined in the CPIA Code (para 2.1 (7)) as material of any kind, including information and objects, which is obtained or inspected in the course of a criminal investigation and which may be relevant to the investigation. It includes material coming into the possession of the investigation but also material generated by the investigation.*

***Relevant Material (CPIA 1996)*** *may be relevant to an investigation if it has some bearing on any offence under investigation or any person being investigated, or on the surrounding circumstances of the case, unless it is incapable of having any impact on the case. (CPIA Code para 2.1(8)). Unless it has been served as evidence, all relevant unused material should be listed on a schedule of unused material.*

Material and Relevant Material gathered or generated by an investigation is likely to include **personal data.**

***Personal Data*** *is defined by section 3(2) and (3) of DPA as any information relating to an identified or identifiable living individual. Identifiable living individual means a living individual who can be identified, directly or indirectly.*

In gathering, retaining, and reviewing personal data as well as disclosing or disseminating this material it is clear that the Police and CPS will be **processing** that information (DPA, s. 3(4)).

The material gathered by an investigation may also involve **sensitive processing**.

*Sensitive Processing is defined in DPA, s. 35(8) as the processing of* ***personal data*** *that reveals racial or ethnic origin, political opinions, religious of philosophical beliefs or trade union membership. It also relates to the processing of genetic data, the processing of health data and data concerning an individual’s sex life or orientation.*

[Part 3 of the DPA](https://www.legislation.gov.uk/ukpga/2018/12/part/3/enacted) establishes six data protection principles. The **first data protection principle** (DPA s. 35) states that the processing of personal data must be lawful and fair. Processing for a law enforcement process is lawful if it is based on law (DPA, s.35(2)) and either the data owner has given consent, or the processing is necessary. It also sets out the additional requirements in relation to **sensitive processing,**

The sharing and disclosure of personal data by the Police and/or the CPS will generally be lawful and fair where this is undertaken in order to:

* establish an element of an offence; the disclosure may be necessary for the CPS to make a charging decision or comply with a continuing duty of review (Annex 3; 4 and 5 of DG6 provide further guidance on what material and information is required);
* explain the context of the offence or offending behaviour;
* enable a case to be presented in a way which gives the court sufficient sentencing powers; or
* comply with CPIA 1996, CPIA Code or other statutory or common law disclosure obligations as part of the organisations law enforcement functions.

It follows that if material or information is either:

* evidence in the case; or
* unused material which meets the test for disclosure

and it includes personal data or sensitive personal data which does not need to be disclosed for a law enforcement purpose, the material or information cannot be sent to the CPS until the personal data or sensitive personal data is redacted from the material or information.

Similarly, the disclosure of personal data from the CPS to the defence or other third party will be lawful and fair if it is necessary and relevant for any law enforcement purpose. This will include service of personal data required as evidence to prosecute a case and the service of personal data that meets the **test for disclosure** under either common law or CPIA 1996.

**Redaction principles relevant to Sensitive Material as defined by the CPIA 1996.**

The other basis for redaction of material relates to **Sensitive Material** as defined by the CPIA 1996. Sensitive Material under the CPIA 1996 is distinct from personal data and sensitive personal data under the DPA. It is material, the disclosure of which would give rise to a real risk of serious prejudice to an important public interest. (para 2.1(9)). Examples of sensitive material can be found at paragraph 6.14 of the CPIA Code.

The existence of relevant sensitive material is revealed to the prosecutor by the investigator / disclosure officer on a schedule of sensitive unused material (MG6D).

Where a relevant document contains a mix of sensitive and non-sensitive material, the sensitive material must be redacted, with a copy of the redacted document placed on the non-sensitive unused material schedule (MG6C) and the original placed on the sensitive schedule (MG6D).

1. **Summary**

Personal data should only be shared or disclosed by the Police / CPS when lawful and necessary. If the personal data is not evidence in the case or required to discharge disclosure obligations under the CPIA 1996 / Common Law, then it should be redacted.

The other basis for redaction of information is under the CPIA 1996. Where a relevant document contains both sensitive and non-sensitive material, the sensitive material must be redacted. The redacted document should be listed on the non-sensitive schedule (MG6C) and the original on the sensitive (MG6D).

Please note that if the CPIA 1996 sensitive material is considered to meet the test for disclosure, then the Police and CPS will need to review and approach that material in accordance with the guidance in the Disclosure Manual.

1. **Escalation Process**

Where there is a requirement to escalate a query in relation to the guidance above the procedures set out in DG6 Part 4 paragraphs 4.31 – 4.34 (charging) and Part 10 paragraphs 10.12 – 10.14 (post charge) should be considered. The latter is replicated below for information.

**Escalation (Director’s Guidance on Charging 6th Edition)**

10.10 The Code[81](https://www.cps.gov.uk/legal-guidance/charging-directors-guidance-sixth-edition-december-2020#reference-81) establishes the concept that a prosecutor’s review responsibilities are continuous, applying throughout the life of a case. The evidential and public interest basis upon which a decision to prosecute is taken may change for a variety of reasons, including the availability or otherwise of evidence arising from the investigation, any view expressed by the complainant, or the receipt of material or information from the defence. Such a change should precipitate a further review.

10.11 It is essential that the police communicate any change in circumstances to the prosecutor as soon as it is known as it may mean the relevant Code Test is no longer met. Further information may also mean that the case is strengthened. Prosecutors must act upon this information as soon as possible, whether upon receipt from the police, the complainant, the defence, or any other source. Failure to progress cases in this way may mean that they proceed without the benefit of material that may strengthen them, that they are prolonged unnecessarily when they should be stopped, or that the court’s expectations around case progression are not met. Resolution of case issues and escalation

10.12 Failing to comply with a request from a prosecutor may place the prosecution in breach of a court direction and imperil the progress or outcome of the case. It is essential that case progression issues between the police and the prosecutor are resolved quickly through an agreed process.

10.13 If any matter requiring a post-charge decision or other action is disputed, or is not completed within an indicative timescale, the police or prosecutor may ask for the issue to be reviewed in accordance with national principles and local arrangements.82 Any such review should take place as soon as possible. If the review cannot resolve the issue(s), it may be further escalated in accordance with the local arrangements. A separate process applies for appeals against charging decisions.[83](https://www.cps.gov.uk/legal-guidance/charging-directors-guidance-sixth-edition-december-2020#reference-83)

10.14 The following general principles are to be applied:

* escalation must be recorded and should explain the rationale for the decision to escalate;
* local escalation policy should involve a minimum of two stages;
* local escalation policy should define the level of decision making required at each stage, and the level of managerial awareness;
* at least seven days should be given for the final stage of escalation unless the relevant timescale for the case does not permit that, in which case the reason must be recorded and shared;
* timescales for any required action should be consistent with the relevant periods set by TSJ and BCM;
* no notice of proposed discontinuance should be served immediately in any case (except minor traffic and other offences with no victim) before the period allowed for escalation has passed, unless the relevant timescale for the case does not permit that.

**Non-Custody Time Limit cases**

|  |  |  |
| --- | --- | --- |
| Request / Escalation stage | Who (CPS) | Who (Police) |
| Initial request for file corrections | Lawyer reviews and requests file corrections giving a 4-day timescale\* for a response | OIC via CJU |
| 1st escalation if no response from OIC | DCP escalates giving a 3-day timescale\* for a response | Local CJ Managers |
| 2nd escalation if items still outstanding | SDCP escalates | Superintendent or equivalent |

\*suggested timescale

**Custody Time Limit Case Escalations**

|  |  |  |
| --- | --- | --- |
| Request / Escalation stage | Who (CPS) | Who (Police) |
| Initial request for file corrections | Lawyer reviews and requests missing items giving a 3-day timescale\* for a response | OIC via CJU |
| 1st escalation if no response from OIC | DCP escalates giving a 2-day timescale\* for a response | Local CJ Managers |
| 2nd escalation if items still outstanding | SDCP escalates | Superintendent or equivalent |

\*suggested timescale

Escalations in relation to ad hoc directions will follow the above principals accepting timescales will be affected by the schedule set by HMCTS.

1. **Review**

This document will be reviewed on an annual basis by NDIP.