

The Disclosure Limitations of the Subject Access Right Provisions - i.e. why the subject access provisions do not provide a complete disclosure process to obtain discovery of documents that may assist a subject access applicant in litigation matters, such as court or complaint proceedings.

The subject access right provisions of the Data Protection Act 2018 (DPA) and the associated General Data Protection Regulation (the GDPR), pertain only to the process of the disclosure of held personal information about the applicant, whereby

- the applicant is the focus of the information within the policing records and reports and/or
- the information is biographical to the applicant, and/or
- the applicant has disclosed/detailed third party information, and/or
- no non-disclosure exemptions are claimed and applied by an organisation, including the police.

The subject access provisions do not enable

- the disclosure of third party personal data not known to the applicant and/or reported directly by the third party; and/or
- a process of answering case enquiries - e.g. questions about actions taken; and/or
- a process of requesting case updates and/or
- the disclosure of information i.e. not personal data – for example police tactics and actions, statistical data etc.

A third party is defined as anyone who is not the subject access applicant.

As detailed within Data Protection 1998 leading test case law (at this time point, there is no leading Data Protection act 2018/GDPR case law) subject access is '*.....not an automatic key to any information, readily accessible or, of matters, in which he may be named or involved.....*'.

Third Party Data i.e. non-applicant personal data & Confidentiality

Under the subject access right provisions of the Data Protection 2018/GDPR, it is not possible to release any personal data and/or information reported to the police by a third party, or any information about a third party in general and/or the police's follow up actions and involvement with any third party, unless the information is already known to the subject access applicant (e.g. the information was reported/provided by the applicant, and/or formed part of an officer case update to the applicant), and/or the consent of the third party is obtained.

Durham Constabulary will not for the purposes of family court or civil court proceedings, employment tribunals or housing applications etc., seek consent from third parties.

In general, Durham Constabulary are statutorily restricted from disclosing third party material i.e. reports of incidents/crimes and safeguarding events, recording of calls, witness allegations or complaints or statements or interview notes etc., as the police owe a duty of care and confidentiality to all third parties, including third party victims, or third party witnesses, or third party suspects, or third party offenders, and any authors of statements under common law. **As you would expect, if a third party applicant submitted a subject access request, Durham Constabulary in the same way would redact and exempt your personal data.**

Clearly it is implicit in the relationship between the police and the third party that the information will only be used for the purpose for which it was originally provided and held i.e. the policing purposes, and not used for a secondary/collateral purpose such as family court or civil court proceedings or housing applications etc. Only with the consent of those who provided the information, or where there is a legal compulsion to make the disclosure (e.g. a court order) and/or under statutory provision (e.g. disclosures to a regulatory authority for safeguarding or financial probity reasons i.e. General Medical Council, Nursing and Midwifery Council, Disclosure and Barring Service, Health & Care Professionals Council, The National College for Teaching and Leadership, The Financial Conduct Authority etc.) or where there is an overriding public interest for the disclosure (e.g. to protect the vulnerable via direct disclosure actions to the Family Court or to statutory safeguarding partners etc., or to protect life etc.) may the duty of care and confidentiality be breached or overridden.

Court Order

Numerous leading test case law has established that third party personal data and/or information given to, or obtained by the police during the course of a police attendance, an enquiry or a criminal investigation or a safeguarding event, is confidential and should not be disclosed for non-policing purposes, such as the subject access right provisions, family court or civil court proceedings, employment hearings, industrial tribunals etc., without the permission of a court or the owner of the .

Case law however also recognises that the duty of confidentiality is not absolute and there are circumstances in which the police can override the duty of confidence owed. Confidentiality may be breached where an opposing interest out-weighs the obligation. Thus, confidentiality will give way to a court order, legal compulsion, or a greater public interest in the disclosure. In general it is accepted that it is best practice for the police to await the receipt of a court request or order before disclosing third party personal data documents to aid family court or civil court proceedings, employment hearings and tribunals etc.

Subject Access Original Documents and Redaction

It is a matter of fact that the subject access provisions of Data Protection Act 2018 do not entitle a person to copies of actual i.e. original documents - for example, original incident reports, crime reports or safeguarding reports, statements, exhibits, evidence or evidential schedules etc. If an original copy documents is however released under subject access rights (as opposed to the legitimate action of extracting only the relevant personal data and pasting it onto a plain paper copy for disclosure purposes), then the copy of the original document will be necessarily, and statutorily redacted to remove non-relevant i.e. third party personal data such as names, addresses and other personal details and/or all other non-relevant information or non-personal data.

Also, a subject access applicant will only receive extracts of materially relevant personal information, whereby the data subject applicant is the focus of the information within and/or the information is biographical to them and/or they have reported personal data about a third party. As detailed earlier, within Data Protection 1998 leading test case law (at this time point, there is no leading Data Protection act 2018/GDPR case law) subject access is *'.....not an automatic key to any information, readily accessible or, of matters, in which he may be named or involved.....'*

Accordingly, this is why the subject access provisions do not provide a complete disclosure process to obtain discovery of documents that may assist a subject access applicant in litigation e.g. family court or other court proceedings, neighbourhood disputes etc., and/or to progress complaints against third parties or organisations.

Accuracy of Records

The Data Protection Act 2018 (and the associated General Data Protection Regulation (the GDPR)) requires that personal data shall be accurate and where necessary kept up to date.

The accuracy principle is however not breached where any organisation has

- accurately recorded professional opinion, observations and actions and/or
- has accurately recorded details from a third party as supplied via telephone or in person or otherwise and/or
- has accurately recorded erroneous information, i.e. where the error or errors originate from the supplier of the information in the first place, either the data subject or from a third party.

The Data Protection Act 2018 and the GDPR covers any expression of opinion about individuals i.e. data subjects. Employers, medical professionals, police officers and police staff, teachers and social workers, among others, will of course routinely record professional opinions. Opinions may be recorded informally or formally in reports, letters, memos, and so on, in a way that is covered by the DPA. It is the responsibility

of each employee to decide what information they need to record to fulfil their business duty (in our case the policing purposes), and they are allowed by the data controller to use their professional judgement to do this. Durham Constabulary's data controller is the Chief Constable.

There is not a definition of 'accurate' in the 2018 Act, nor does the GDPR define the word 'accurate', however, the DPA 2018 (and this was also the case for the DPA 1998) does say that 'inaccurate' means "incorrect or misleading as to any matter of fact".

For the purposes of the Data Protection Act 2018 and the GDPR, personal data is therefore inaccurate, if the information is incorrect or misleading as to any matter of fact. An opinion is not classified as a matter of fact, unless the opinion given is presented (within the personal data) as a matter of fact – e.g. *'it is a matter of fact that X is cheeky or arrogant'* etc. An opinion is therefore classified as a statement of opinion rather than a matter of fact. Opinions are naturally subjective, and will depend on the experiences and understanding and observations of the individual concerned. The fact that someone i.e. the data subject or someone else of their behalf i.e. a solicitor etc., might hold a different opinion or obtains a second professional opinion, which then contradicts the first opinion, does not then make the first opinion inaccurate and require deletion.