

## **Question 1.2**

### **Evidence of Harm**

Inappropriate disclosure of information about an investigation can interfere with that investigation by allowing suspects to change their behaviour, destroy evidence or prepare alibis based on their knowledge of the information known by West Midlands Police.

Release of information through the Freedom of Information Act removes any of the legal strictures and assumptions of confidentiality associated with the due legal process. As a consequence any on-going or subsequent court proceedings could be jeopardised where release of information regarding an individual was identified.

### **Public Interest Considerations**

#### **Section 30 (1)(a)**

##### **Factors favouring disclosure**

Disclosing information about investigations would provide a greater transparency in the investigating process and the actions of a public authority. It is clear that there is a public interest in public authorities operating in as transparent a manner as possible, as this should ensure they operate effectively and efficiently.

##### **Factors against disclosure**

There is an inherently strong public interest in public authorities carrying out investigations to prevent and detect crime. This ensures that offenders are brought to justice and that the necessary checks and balances are in place to safeguard public funds and resources. To allow the effectiveness of investigations to be reduced, as described in the harm above, is not in the public interest.

It would not be in the public interest to provide information that may be of assistance to offenders/prevent an individual from being brought to justice. The right to a fair trial is of paramount importance and any disclosure which could enhance media attention prior to any proceedings could compromise an individual's right to a fair trial under the Human Rights Act.

#### **Section 31(1)(g)**

##### **Factors favouring disclosure**

There is a clear public interest in ensuring that public authorities do not act outside their authority by investigating matters which fall outside their remit. By making certain that public authorities provide information in relation to investigations, this should provide the necessary safeguards and satisfy the public interest in this matter.

### **Factors against disclosure**

Where current or future professional standards role of the force may be compromised by the release of information, then this is unlikely to be in the interest of the public. In this case, for the reasons outlined above, providing details of an investigation could jeopardise future police investigations.

The interest of the public is best served by the non-disclosure of information which adversely affects the reputation of an individual e.g. whether they are involved in a police investigation. In this case the request specifically asks for information about individuals.

### **Balancing Test**

For a public interest test, issues that favour release need to be measured against issues that favour non-disclosure. The public interest is not what interests the public, or a particular individual, but what will be the greater good, if released, to the community as a whole.

The issue of transparency is noted. However, on balance it is considered that the public interest in providing the information exists is outweighed by the potential impact release would have on individual's privacy and on future investigations.

Although provision of the requested information might provide a greater transparency in the investigating process, there are already a number of checks and balances on authorities to assess whether investigations are conducted appropriately. There are legal processes in place to ensure that all parties are given access to all the appropriate information at the time of any trial and subsequently through court records. In addition if a person feels that they have been treated inappropriately by the police there are clear processes in place to ensure that matters are investigated thoroughly and appropriately.

Releasing information outside of such a schedule could undermine the smooth running of these processes and would impact on future judicial proceedings. Therefore the wider public interest lies in protecting the ability of the public authority to conduct an effective investigation and consider the outcome.

Having considered the arguments for and against, the public interest test favours withholding the information. West Midlands Police will not disclose information that could reveal personal information or could compromise the future law enforcement role of the force.

### **Question 3**

#### **Evidence of Harm**

Policing is an information-led activity, and information assurance (which includes information security) is fundamental to how the Police Service manages the challenges faced. In order to comply with statutory requirements the College of Policing Authorised Professional Practice for Information Assurance has been put in place to ensure the delivery of core operational policing by providing appropriate and consistent protection for the information assets of member organisations, see below link:

<https://www.app.college.police.uk/app-content/information-management/>

To confirm or deny whether cyber security incidents have occurred would identify vulnerable computer systems and provide actual knowledge, or not, that these incidents have taken place within individual force areas.

In order to achieve this goal, it is vitally important that information sharing takes place with other police forces and security bodies within the UK to support counter-terrorism in the fight to deprive terrorist networks of their ability to commit crime.

To confirm or deny specific details of any cyber security incident would be extremely useful to those involved in terrorist activity as it would enable them to map vulnerable information security databases.

#### **Public Interest Considerations**

##### **Section 24(2) National Security**

##### **Factors favouring complying with Section 1(1)(a) confirming that information is held**

The public are entitled to know how public funds are spent and how resources are distributed within an area of policing. To confirm whether cyber security attacks have occurred would enable the general public to hold West Midlands Police to account ensuring all such breaches are recorded and investigated appropriately. In the current financial climate of cuts and with the call for transparency of public spending this would enable improved public debate.

##### **Factors against complying with Section 1(1)(a) confirming or denying that information is held**

Security measures are put in place to protect the community we serve. As evidenced within the harm to confirm where cyber security attacks have occurred would highlight to terrorists and individuals intent on carrying out criminal activity, vulnerabilities within West Midlands Police.

Taking into account the current security climate within the United Kingdom, no information (such as the citing of an exemption which confirms information pertinent to this request is held, or conversely, stating 'no information is held') which may aid a terrorist should be disclosed. To what extent this information may aid a terrorist is unknown, but it is clear that it will have an impact on a force's ability to monitor terrorist activity.

Irrespective of what information is or isn't held, the public entrust the Police Service to make appropriate decisions with regard to their safety and protection and the only way of reducing risk is to be cautious with what is placed into the public domain.

The cumulative effect of terrorists gathering information from various sources would be even more impactful when linked to other information gathered from various sources about terrorism. The more information disclosed over time will give a more detailed account of the tactical infrastructure of not only a force area but also the country as a whole.

Any incident that results from such a disclosure would, by default, affect National Security.

### **Section 30(3) Investigations**

#### **Factors favouring complying with Section 1(1)(a) confirming that information is held**

Confirming or denying whether information exists relevant to this request would lead to a better informed general public by identifying that (force name) robustly investigate cyber security incidents. This fact alone may encourage individuals to provide intelligence in order to assist with investigations and would also promote public trust in providing transparency and demonstrating openness and accountability into where the police are currently focusing their investigations.

The public are also entitled to know how public funds are spent, particularly in the current economic climate.

#### **Factors against complying with Section 1(1)(a)**

Modern-day policing is intelligence led and (force name) share information with other law enforcement agencies as part of their investigation process. To confirm or not whether (force name) has alerted other agencies of cyber security attacks could hinder the prevention and detection of crime as well as undermine the partnership approach to investigations and enforcement.

Should offenders take evasive action to avoid detection, police resources may well be diverted from frontline duties and other areas of policing in order to locate and apprehend these individuals. In addition, the safety of individuals and victims would also be compromised.

### **Section 31(3) Law Enforcement**

#### **Factors favouring complying with Section 1(1)(a) confirming that information is held**

Confirming that information exists relevant to this request would lead to a better informed public which may encourage individuals to provide intelligence in order to reduce these attacks.

**Factors against complying with Section 1(1)(a) neither confirming nor denying that information is held**

Confirmation or denial that information is held in this case would suggest West Midlands Police take their responsibility to protect information and information systems from unauthorised access, destruction, etc., dismissively and inappropriately.

**Balancing Test**

The points above highlight the merits of confirming or denying the requested information exists. The Police Service is charged with enforcing the law, preventing and detecting crime and protecting the communities we serve. As part of that policing purpose, information is gathered which can be highly sensitive, relating to high profile investigative activity.

Weakening the mechanisms used to monitor any type of criminal activity, and specifically terrorist activity would place the security of the country at an increased level of danger.

In order to comply with statutory requirements and to meet NPCC expectation of the Police Service with regard to the management of information security, a national policy approved by the College of Policing titled National Policing Community Security Policy has been put in place. This policy has been constructed to ensure the delivery of core operational policing by providing appropriate and consistent protection for the information assets of member organisations. A copy of this can be found at the below link:

<http://library.college.police.uk/docs/APP-Community-Security-Policy-2014.pdf>

In addition anything that places that confidence at risk, no matter how generic, would undermine any trust or confidence individuals have in the Police Service. Therefore, at this moment in time, it is our opinion that for these issues the balance test favours neither confirming nor denying that information is held.