

## FOI unit keeps us ahead of the game

The FOI unit is responsible for making sure the force complies with current legislation. All FOI requests made to the force are answered by the central team, ensuring they do not interfere with the day-to-day running of OCUs and departments.

Steve Mountford, manager of the FOI Unit, said: "The unit allows consistency and corpora- cy to be applied to all responses as well as the correct applica- tion of the legislation – which can be a complex process.

"The obligation to comply with the FOI Act's requirements carries equal weight to the force's core functions of reducing and detecting crime.

"In the near future, compliance with the Act will form part of the HMIC's baseline assess- ments of the force.

"To ensure harmful informa- tion is not inadvertently released or unlawfully withheld, it is important that the FOI Unit sees all information released under the Act.

"The unit has experience and expertise and is better placed to understand the legislation, and also the need to liaise with other stakeholders such as other forces, councils or government departments.

"Ill-considered responses would not only poorly serve the public, but could also result in WMP being issued with an enforcement notice.

"All requests made under the Act should be forwarded to the unit without delay, as we are required to answer them within a relatively short space of time."

## When and why we say No

THERE are a number of legiti- mate reasons why information may be withheld under FOI. If this is the case, the legal rea- son for not releasing the data must be communicated to the requester.

If the information falls into any of the following categories, it may be withheld:

- It is accessible to the applicant by other means
- National security
- Investigations conducted by public authorities
- Law enforcement
- Court records
- Health and safety
- Personal information
- Information provided in confi- dence
- Legal professional privilege
- Commercial interests

One of the main reasons why information may be withheld is that it is personal data – if a per- son asks for information about themselves the request will be handled under the Data Protection Act.

Although requests under FOI are free, if it costs more than £450 to find the information and prepare it for release, then the request can be turned down.

# Acts open the door for public to seek information

**O**PEN, honest and accountable – those are the principles behind giving the public access to information held by the police.

Anyone anywhere can make a written request for information held by the force. If the information relates to an individual it will be answered under the Data Protection Act, if not it will be answered under the Freedom of Information Act.

A dedicated team of eight people based at police headquarters receives, process- es and tracks public requests and ensures people are given the right answers to their questions.

While people have the right to request information, there are restrictions and exemptions on what the force can provide.

The Data Protection Act is designed to

**P**OLICE forces are used to keeping information confidential but two acts allow the public access to more information held by the police than ever before. **Samantha Bates and Hilary Hopker** look at how the Data Protection and Freedom of Information Acts impact on the force and, at the team who process public requests for information

let individuals apply for information which may be held about them and gives them the opportunity to correct that information.

Most people applying for information about them from the force are doing so

because they need proof of their police record when applying for a travel visa, they are being vetted or they need the information from incident logs for civil proceedings.

Kate Firkins, Data Protection Manager said: "Information is one of our major assets. Everyone is responsible for its accuracy, integrity, availability and confidentiality. If you record a personal comment about someone on computer or in a paper file, that person now has the right to apply for a copy of it."

The Freedom of Information Act was brought in to increase openness and transparency within public authorities. It is hoped over time the Act will increase public trust in the police and improve the relationship between the force and the community.

For help and support you can contact the Data Protection and Freedom of Information team on ext 7800 2070.



# The inform

## How many dogs does the force have?

HERE are 10 of the more inter- esting questions the team has received:

- Has the force ever used psy- chics to solve murders?
- Is there any information about an incident in the early 1980s, classified as an 'inexplicable event', when a number of houses were damaged by falling stones?
- Are there any regulations about the percentage of light transmissions of the tint of car windows?
- How many crimes are com- mitted on farms?
- Has there been an increase in the number of criminals wearing gloves at crime scenes?
- How many reports of sightings of escaped wild/exotic animals have there been since 2000?
- How much have hunting-relat- ed inquiries cost since the Hunting Act came into force?
- How many dogs are currently employed by the force?
- Are there new rules regarding dogs travelling in vehicles?
- Is it illegal to own and carry your own handcuffs if you are not a police officer?

The answers to some of these queries and many other frequen- tly asked questions can be found on the Police National Legal Database's website, located at [www.askthe.police.uk](http://www.askthe.police.uk).



## Press and public clamour to know

**TWENTY** per cent of FOI requests made in the UK made to police forces can receive the second highest number of requests of any force in the country.

Almost half of the FOI requests the force receive are from members of the press, a rise from the general public around 16 per cent are made by students.

About a third of all requests are for information about across the force area.

Other commonly requested areas of information are about data, policies and procedures, finance and human resources. The Freedom of Information Act can be a useful news-gathering tool for the media. FOI requests can reveal worthy material that would

## Handle this stuff with care – here's why even

**BREACHING** the Data Protection Act could lead to criminal proceedings. Police officers and staff have been prosecuted for obtaining and disclosing personal information unlawfully.

Members of the force must only use or access information they need to carry out their current duties.

Most problems occur when people look up information for a personal purpose, such as run-

ning a PNC check on their daughter's new boyfriend, or search force systems merely because they are bored or curious.

National examples of cases where officers and staff have

faced prosecution after breach- ing the Data Protection Act include:

● A police officer who gave a friend details of his estranged wife's new boyfriend, which were then used to track down



### Information is important, so handle with care

OFFICERS and staff handle personal information on a daily basis and it is crucial they deal with it correctly.

The Data Protection Act sets out how information should be obtained, processed and stored. Enacted in 1998, the Act applies to living people and covers information held about them on computer and within paper files.

At the heart of the Act are the eight Data Protection principles, which are common sense rules for the use of personal information.

They state that personal information must be:

- Fairly and lawfully processed

- Processed for limited purposes

- Adequate, relevant, not excessive

- Accurate

- Not kept for longer than necessary

- Processed in accordance with rights of individuals

- Secure

- Not transferred to countries without adequate protection

Management of Police Information (MoPI) follows the same principles as the Data Protection Act. If you comply with MoPI you will be complying with Data Protection legislation.

### Facts that you can release to public

THERE are some common misconceptions about what information is prevented from being released under the Data Protection Act.

The Act does not prevent the release of:

- A crime reference number, once a caller's identity has been verified they are entitled to a crime number
- Photographs of offenders and suspects. In certain circumstances it is in the public interest for photographs to be made available for the purpose of crime prevention or detection, providing these circulations are purposeful and reasonable
- Information to partner agencies; where personal information is regularly requested and shared, an Information Sharing Agreement would be required. It is always necessary to ensure the sharing is in accordance with a legal power; without a legal power it is not possible to share information lawfully
- Victim's details being given to Victim Support; officers need to make it clear to the victim that their details will normally be passed on to Victim Support unless they ask for them not to be

# Information jungle

nd  
r  
v

DI  
K are  
nd WMP  
est num-  
er in

requests  
on  
third  
ibic and  
sent in

quests  
ut crime

sted  
person-  
cedures,  
ures.  
ation  
s-gath-  
il news-  
uld oth-



otherwise have remained secret, or provide depth and background to ongoing issues.

Media requests have resulted in a number of headlines covering such diverse topics as:

- 1,000 police cells for Merry Hill

- Black Country crime hotspots named
- 130 police officers quit West Midlands force
- Police landed with £43,000 repair bill
- Cannabis factory numbers treble

## Sometimes we need help from outside – and it's not always plain sailing

GETTING information from other organisations to help with police enquiries is never easy.

The Data Protection Act allows organisations to release information lawfully to the police if it can be proved the information is needed for the prevention or detection of crime or the apprehension or prosecution of offenders.

Form WA170 on the standard forms section of the intranet can be used for this purpose. However, if the organisation still refuses to hand over the information, officers will have to seek a court order.

There are also times when the force needs to share its information with other agencies.

The disclosure issue is a complex one which is not easily understood but could lead to unlawful information sharing or a lack of co-operation if officers do not understand it. When there is no duty to disclose informa-

tion but relevant powers exist such as section 115 of the Crime and Disorder Act, an information sharing agreement is required.

This creates a clear understanding as to what information can be shared, how, with whom, and for what purpose.



The disclosure issue is a complex one which is not easily understood

There are three types of disclosure:

- Information required by statute, eg court order, request from CSA

- Where there is a statutory power, eg S115 of the Crime and Disorder Act. Disclosure is discretionary and the force is not compelled to share information

- Where the disclosure is to support the policing purpose – a pressing public interest and it

is relevant and proportionate to do so. If of these categories, it probably breaches data protection and should not be considered.



Victims' details will normally be passed on to Victim Support unless they ask for them not to be

## Requests up year after year

THE number of requests processed by the force's Data Protection and Freedom of Information department has steadily increased.

- The Data Protection team handled:  
● 6,951 requests in 2004  
● 7,156 requests in 2005  
● 7,748 requests in 2006

The Freedom of Information team handled:

- 832 requests in 2005  
● 1,039 requests in 2006  
● 241 requests in the first quarter of 2007

Requests can take anything from one hour for simple queries to a maximum of 18 hours to deal with.

The force doesn't have to meet any requests taking more than 18 hours.

## Police officers and staff may end up breaking the law

the man and assault him

- A police officer who passed information from the Police National Computer (PNC) about car registration details to criminal friends, who then used that information to kidnap and

blackmail a businessman

- A member of police staff who got details of her ex-boyfriend's new girlfriend via a check on a car outside his house, because she wanted to know who he was seeing

- A police officer who passed a hotel manager details of his staff's criminal records in exchange for free hotel accommodation

- Police officers who passed information from the PNC on to

a private detective agency

- An officer who illegally accessed information on his wife's new boyfriend and sent him a series of false fixed penalty notices
- Two police officers who

tipped off a criminal that he might be the subject of an undercover operation

- A chief inspector who looked up the address of a former colleague he held a grudge against in order to issue him with a writ