

Crime-mapping and geo-spatial crime data: privacy and transparency principles.

- **Transparency should be the default position regarding information about crime location. Information about crime location should be available to the public, unless there is a risk of damage or distress, especially to victims, witnesses and those reporting crime.**
- **Where there are no risks, or they are minimal, crime maps and allied data disclosures should provide as much information as possible, to enable the public to understand crime in their area. This can also enable communities to engage with agencies such as the police and bring about enhanced accountability.**
- **It is legitimate to give victims of crime access to more detailed information about crimes involving them than members of the general public should be given.**
- **Publishing exact household level mapping pins on crime maps will generally constitute the processing of personal data and is likely to breach the first data protection principle's requirement of fairness. This is because it is quite easy to link a crime to a property and a property to its occupant or occupants – using the publicly available Electoral Register for example.**
- **The use of heat maps, blocks and zones can help to represent crime location and type in a way which reduces privacy risks. A strong public interest case would have to be made for the use of more granular or intrusive indicators.**
- **Privacy risk depends on the frequency of publishing crime data and the way it is represented and categorised. Where real-time or very frequent publication takes place, it becomes easier to link police activity to an individual and to a crime type. Publishing data very frequently or in real-time poses a greater privacy risk.**
- **Local knowledge might mean that even where a map is published in a privacy-friendly way – for example by mapping against relatively large geographical areas – it may be possible to link a victim to a crime-type. This means that great care must be exercised in publishing**

data about crimes whose publication may lead to harm or distress to victims.

- **The larger the number of properties or occupants in a crime-mapping area, the lower the privacy risk.**
- **As experience of crime-mapping develops, new ways of representing information about crime should be explored. The aim should be to minimise privacy risk whilst making crime-maps more accurate, dynamic and meaningful to the public.**
- **The Information Commissioner recognises the general popularity of crime maps and their potential value to the public. Crime maps can serve various purposes, for example showing basic crime location data, providing information about the progress of an investigation and assisting with victim support. The use that is made of the different features of crime-maps should be reviewed periodically by those publishing them. If the evidence shows that some features of crime-maps are not being used, alternatives to including them should be explored, particularly where high risk types of data are involved. Different types of data disclosure or local publicity might be alternatives.**

Crime-mapping, geo spatial crime data, privacy and transparency: advice from the Information Commissioner's Office.

Crime-mapping is the process of producing a geographical representation of crime levels, crime types or the locations of particular incidents. The main crime mapping service in the UK is www.police.uk, but various local initiatives and pilots are underway. Alongside the crime mapping service there is also impetus to disclose geo-spatial crime data in open formats, enabling third parties to carry out their own mapping and data analysis. The Information Commissioner welcomes and supports the move to make more information available to the public in open formats, provided that privacy safeguards are in place.

Crime-maps can give citizens a readily accessible means of understanding patterns of crime in their area. It can help them to evaluate the priorities and performance of the police and to make informed judgements pertinent to their safety and well-being. The Information Commissioner fully recognises the value of this. He will use his powers and duty to promote good practice to ensure that the availability of crime data becomes an established part of the public's 'right to know' and that the private lives of victims and others are respected.

It is important to look at crime-mapping in its wider social context, particularly in relation to societal expectation of both privacy and transparency – including the principle that justice must be seen to be done. Long-standing rules relating to the confidentiality and protection of victims and witnesses must be taken into account. The Press Complaints Commission's 'Editors' Code of Practice' contains rules relating to the identification of crime victims, witnesses and perpetrators¹. The Code of Practice for victims of crime establishes victims' rights². The UK Statistics Authority's Code of Practice for Official Statistics contains a confidentiality principle requiring that official statistics do not reveal the identity of an individual or any private information relating to them. The Information Commissioner will take these privacy conventions into account when assessing whether the publication of a particular crime-map, or release of data, is in compliance with the first data protection principle's requirement that personal data shall be processed fairly.

Crime-mapping is, by definition, concerned with the geographical aspects of criminality. However, it can have an impact on

¹ <http://www.pcc.org.uk/cop/practice.html>

² http://www.cps.gov.uk/victims_witnesses/victims_code.pdf

individuals' privacy where a link can be established between a crime, a location and an individual - allowing identification to take place.

The purpose of these guidelines is to help those involved in crime-mapping or other data release to assess and minimise the privacy impact of their activity. In particular, these guidelines are intended to protect individuals, primarily victims, witnesses and reporters of crime.

Crime-mapping and personal data.

Crime-mapping takes different forms and does not always involve the processing of personal data. However, in some cases it will. The most obvious example is a pinpoint on a crime-map showing that an incident took place at a particular domestic property. Usually, information like this should only be published with the consent of the person that inhabits the property, given the high risk of identification. An exception would be where the details of a crime have already entered into the public domain.

Given variations in the occupancy of domestic properties, those publishing crime data may not know whether information about a domestic property relates to one person – a single occupant – or to a group of people (multiple occupancy). Publishers may have no way of finding this out. Therefore, in this context, the Information Commissioner recommends that, as a matter of good practice, information linked to a specific domestic property is treated as though it were personal data.

What purpose does crime-mapping serve?

Crime-mapping in the UK is relatively new. It is not yet clear how, or to what extent, the general public uses crime-maps or third parties use crime data. The use that is made of crime maps has implications for their design. For example, if individuals want to use crime maps to safeguard their personal safety – for example by avoiding areas with a high level of street robberies – then clearly a geographical representation of crime would be appropriate. However, if individuals want to find out how effective their local police force is in apprehending and prosecuting street robbers, for example, then a different form of representation might prove more useful – for example statistical data about rates of apprehension or prosecution.

The purpose of crime-mapping also has implications for the type of crimes that are shown on a map. For example, it is difficult to see

how providing information about the location of domestic violence incidents will help members of the public to avoid areas of danger. However, it may be justified to publish information about the scale of domestic violence, or police success in dealing with it, in some other form, for example statistical.

Publishing data about crime can present varying degrees of privacy risk, depending on how it is done. Any degree of risk must be justified through the availability of evidence as to the purpose and effect of crime-mapping. Levels of usage of crime mapping websites or downloads of crime data should be monitored by those publishing data, and if usage is low a review should take place. The Commissioner would encourage further research to be commissioned by those publishing data to assess the impact of crime mapping and allied crime data disclosures.

Because this is a relatively new and innovative area, the Commissioner notes that it may take some time for benefits as well as privacy risks to emerge. It is vital that there is a rolling evaluative process. Any further research by organisations carrying out crime mapping or publishing other data should give due weight to privacy risk.

Areas, numbers and population density.

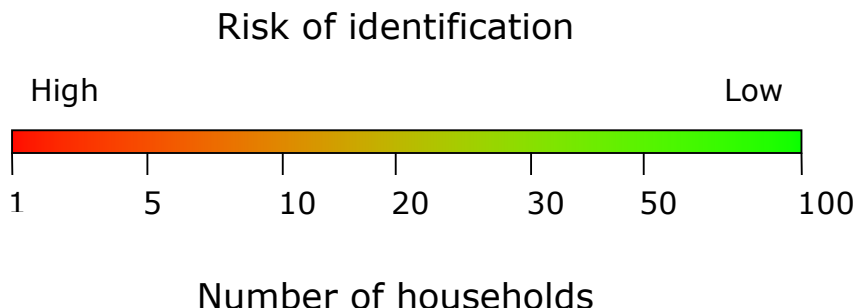
The chance of an individual being identified diminishes as visual granularity decreases – for example where crimes are mapped against policing beats or administrative areas. As the areas indicated on a crime-map grow larger, the risk of an individual being identified in relation to a particular crime grows smaller.

The Information Commissioner will take the following factors into account when assessing whether the processing of personal data done as a result of the publication of a crime-map complies with the Data Protection Act 1998 (DPA):

- the granularity of the crime-map or data
- the regularity of data uploads
- the sensitivity of the crime
- the information recorded on the map
- the availability of other sources of information, and
- the effect on victims and others

The Information Commissioner expects organisations to carry out a privacy impact assessment (PIA) to help them assess these factors³. This should take place early on in the planning process.

The statistical issues underlying the privacy aspects of crime-mapping are complex. They depend primarily on the number of properties in a mapping area and the number of residents of a property. The greater the number of individuals (number of properties X number of residents) in a mapping area, the lower the privacy risk.



The sensitivity of a crime must also be taken into account. The privacy threshold for publishing information about relatively non-sensitive crime, such as car theft, is lower than that for publishing information about sensitive incidents, such as an assault or 'hate-crime'. In these more sensitive scenarios certain individuals or groups will often have greater motivations to seek to identify victims. In assessing compliance with the DPA, particularly fairness, the Information Commissioner will consider the nature of the crime as well as the technique used to map it.

Indicating crime scenes and levels on crime maps

There are various ways of presenting information on crime-maps. The most privacy invasive is to link a particular crime to a particular property using household pinpointing. There is a relatively high risk that this could lead to the identification of an individual. For this reason, the Information Commissioner does not favour the use of household pinpointing on crime-maps.

Approximate crime location indicators can be used, but this can be misleading because the pinpointing of a particular property may be meant to indicate that a crime took place within the general area. Similar problems can occur where an approximate crime location

³

http://www.ico.gov.uk/for_organisations/data_protection/topic_guides/privacy_impact_assessment.aspx

indicator is placed at the 'average' centre of a postcode area, for example. This can lead to properties in the middle of the postcode being shown to be high crime areas when this is not the case. This type of mapping technique can be acceptable provided the meaning of the indicators on the maps is explained properly.

If approximate location indicators are to be used on a crime-map, it should be made clear this merely indicates the area in which a particular crime took place and not the actual location of a crime. A clear, prominent explanation of the pinpoints, other indicators, symbols and so forth used on a crime-map should be provided, to minimise the risk of individuals misinterpreting it.

Publishing crime reference numbers.

Publishing reference numbers such as police Unique Reference Numbers (URNs) or Crime Reference Numbers (CRNs) on crime maps can allow individuals such as the victim of a crime, or the person that reported it, to track 'their' crime and to find out, for example, the result of the police's investigation. It can also allow members of the general public to track crimes they are interested in. This clearly has significant transparency advantages.

However, caution must be exercised when publishing reference numbers. In particular, the availability of information allowing the linkage of a number to an explicit identifier, such as a person's name and address, must be assessed. As well as the police, organisations such as insurance companies and local authorities may hold both numbers and explicit identifiers. URNs or CRNs can also be used for different purposes. For example, in one area the URN/CRN can be used as the log in for victims/witnesses to track their crimes whereas in another area the URN/CRN could be more widely available to enable members of the public to contact the police to provide further information in relation to a specific crime. The risk of identification of victims could be reduced by publishing incomplete numbers or generating different numbers solely for crime-mapping purposes.

Non-residential premises.

Privacy risks arise when crime-mapping domestic properties because of the possibility of associating particular properties with their owners or inhabitants. The degree of risk is lower when crime is mapped in relation to non-residential properties such as pubs, schools, shops or factories.

Crime-mapping may make a direct link between a crime and a particular property, for example a shop. This could allow a connection to be made between a crime and an individual involved in it, for example the proprietor of the shop. However, even where this is the case the privacy risks are not as great as when domestic properties are mapped. This is because running a school or a pub, for example, is an essentially public activity and does not engage the same level of privacy protection as an individual's private life. This will be reflected in the Information Commissioner's approach to the mapping of crime in relation to non-residential premises. However, organisations publishing crime maps that link crimes to non-residential premises should still take account of the risks to individuals that might arise when deciding how, or whether, to publish information. Particular care must be taken where non-residential and residential premises exist in the same building.

Public spaces.

Mapping crime in relation to public spaces will generally pose a low privacy risk. This is because there is very little chance of a car-park or area of wasteland, for example, being associated with a particular individual. Where a map records multiple instances of anti-social behaviour at a location, it will be even more difficult to link crime-mapping data to a particular individual. Again, the relatively low privacy risk that arises here will be reflected in the Information Commissioner's approach.

Publishing sentencing details of individuals and images of offenders and others.

There is a general consensus that images of victims or witnesses should not be published without their consent, particularly where sensitive crimes are involved. The Information Commissioner shares this view. However, the situation is less clear regarding the publication of images of those accused or convicted of offences. Publishing images of identifiable individuals constitutes the processing of personal data, and this activity must therefore be done in compliance with the Data Protection Act 1998. This means that the publication of any image must be *necessary* for a specific purpose.

Publishing images of those involved, or thought to be involved, in crime could be justified where, for example, it is necessary to:

- bring about the apprehension of an offender,
- alert the public that an individual has been excluded from a particular geographical area as part of an ASBO or that a

- particular individual is at large and may be guilty of a crime, or
- alert the public that an individual has been sentenced for a significant offence

In the Information Commissioner's view it is difficult to justify the publication of images where this is only done to satisfy public curiosity. However, the Information Commissioner recognises that for the purposes of restorative justice, the victims of crime should be allowed greater access to information about their assailants, including images of them – this may well come about as part of the judicial process anyway.

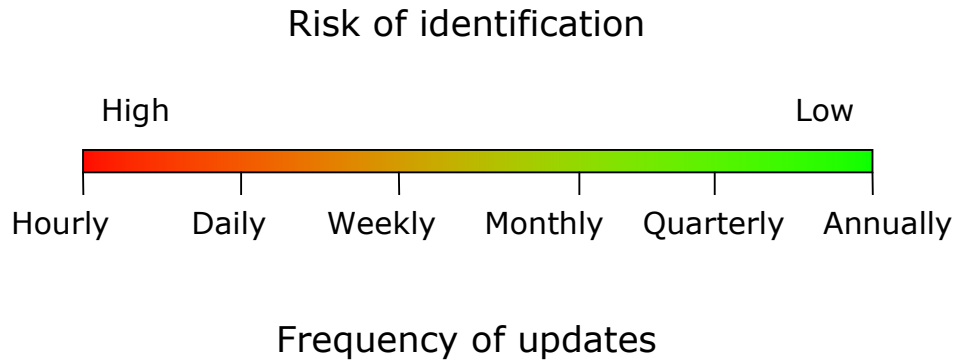
If sentencing details and images of offenders are published, the period of publication should be justified. Thought needs to be given to the ability of others to re-use data or images and to conditions of re-use. In reality, once published, it may be impossible to control further use, disclosure or retention of an image – meaning that the initial publication of the image must be done with due care.

It is also important to consider the broader effect of publishing images of individuals, for example in terms of the rehabilitation of offenders. The CJS' Publicising Sentencing Outcomes guidance⁴ for public authorities touches on these issues.

Timing

The frequency with which data is uploaded to a crime-map has privacy implications. It would be relatively easy for an inquisitive local resident to find out that the police had visited a neighbouring property in response to a particular type of incident if the data is uploaded in real-time or very frequently. The privacy risk declines the less frequently the data is uploaded. Again, avoiding the use of household pinpointing provides additional protection to individuals.

⁴ <http://www.justice.gov.uk/downloads/guidance/sentencing-outcomes/publishing-sentencing-outcomes-guidance.pdf>



Raw crime datasets.

Crime-mapping is just one way of releasing information about crime. Another way is to make data downloadable in a statistical form. Whilst this may prevent some of the problems associated with the interpretation of crime maps, the release of crime statistics can lead to similar privacy concerns and suitable privacy safeguards must be in place. For example, data should be expressed in blocks, based on ranges of grid references, rather than on exact map references. The 'granularity' considerations are broadly the same as those that arise when creating a crime-map.

Other sources of information

When publishing a crime-map you need to be aware of other sources of publicly available information that could be combined with a crime-map to allow the identification of individuals. Obvious examples include:

- newspaper crime reports
- the electoral roll
- online street-maps
- postings on social networks and other sites

It is also important to recognise that increasingly sophisticated 'data mashing' techniques make it easier for the general public to combine information resources to produce a richer, and possibly more privacy-intrusive, picture of crime in their area.

Taking into account the local knowledge of individuals can be particularly problematic. On the one hand, the privacy risks of crime-mapping might be relatively low because a neighbour or someone living in the same street already saw, or has found out, what went on at a particular place at a particular time. On the other hand, a combination of local knowledge and published crime data might allow an individual to find out that a neighbour was subject to

a particular type of crime – something the neighbour might not have wanted to be revealed, especially if the crime was sensitive.

The consequences of crime-mapping.

Crime-mapping is relatively new, and its implications for individuals and for society more widely are not yet fully understood. In particular, there is still no general consensus as to the degree of granularity that strikes the right balance between social transparency in respect of criminality and the privacy of those associated with a crime. For this reason it is very important to monitor whether the publication of a crime-map is having any negative effect on the local community, for example by facilitating repeated victimisation or the harassment of witnesses or complainants. It is also important that risks of identifiability from certain types of crime data are kept under review as new sources of information enter the public domain. Numbers of complaints related to alleged identification via crime maps should be logged and monitored. The Information Commissioner recognises, though, that the knowledge of local criminals could be considerably more useful than a properly drawn-up crime-map – for example when carrying out repeated burglaries. Similarly, crime reports in local newspapers can identify the victims and perpetrators of crime more directly than any crime-map.

Secondary uses of crime-maps

Crime-maps clearly have a range of secondary uses, for example to estate agents or insurance companies. The data supporting crime maps will often be made available and in reality, the publisher of a crime-map may be powerless to prevent secondary uses of the data recorded on it once it has gone into the public domain. However, third parties collecting and using data from crime-maps for their own purposes will take on their own data protection responsibilities and liabilities, if they or others can identify individuals from the data. Personal data is not 'fair game', even if it is already publicly available.

The public utility of crime-mapping and alternatives to it.

It is good practice – and may be a legal requirement where personal data is involved – to find out whether, or how, members of the public and third party developers are using crime-maps and other published data. This could be done through the use of online questionnaires, or by analysing web traffic to find out how a site is being used and whether individuals revisit it. It will be difficult to justify increasing risks of identification if levels of usage are low and

the benefits are unclear. The Commissioner also acknowledges that it may take some time for both risks and benefits to emerge, therefore a rolling programme of evaluation is vital.

Despite the apparent popularity of crime-maps, it may be more useful for the public, and more privacy friendly, to use some types detailed of data about crime to target crime awareness campaigns at areas where there are particular problems. For example, residents of area that are being targeted by burglary gangs could be leafleted with advice about household security. This could be done electronically where individuals have provided their contact details.

Even where a crime map is withdrawn - for whatever reason - the DPA would not prevent archived versions of it being retained and made available for use for purposes such as historical research or statistics.

Victims and the general public – giving the right level of access to information.

Victims and members of the general public can have different degrees of access to information about crime. A failure to recognise this can lead to:

- victims of crime being denied access to information that has real significance for them on spurious privacy grounds, or
- members of the general public being given too much access to information about crimes that have not affected them personally.

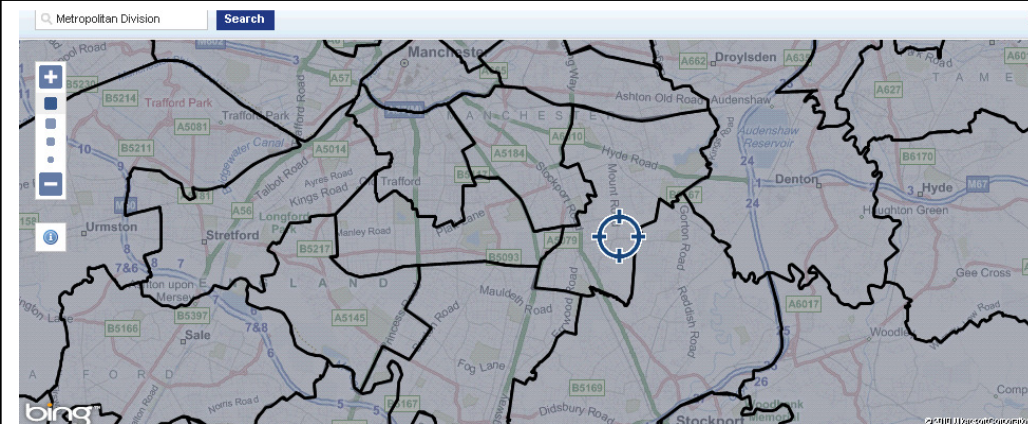
It is generally legitimate to give victims of crime access to more detailed information about their case than the general public should enjoy. This can be facilitated by giving victims protected access to a secure website where they can track the progress of their case by entering an identification credential or crime number, for example.

Redress for individuals

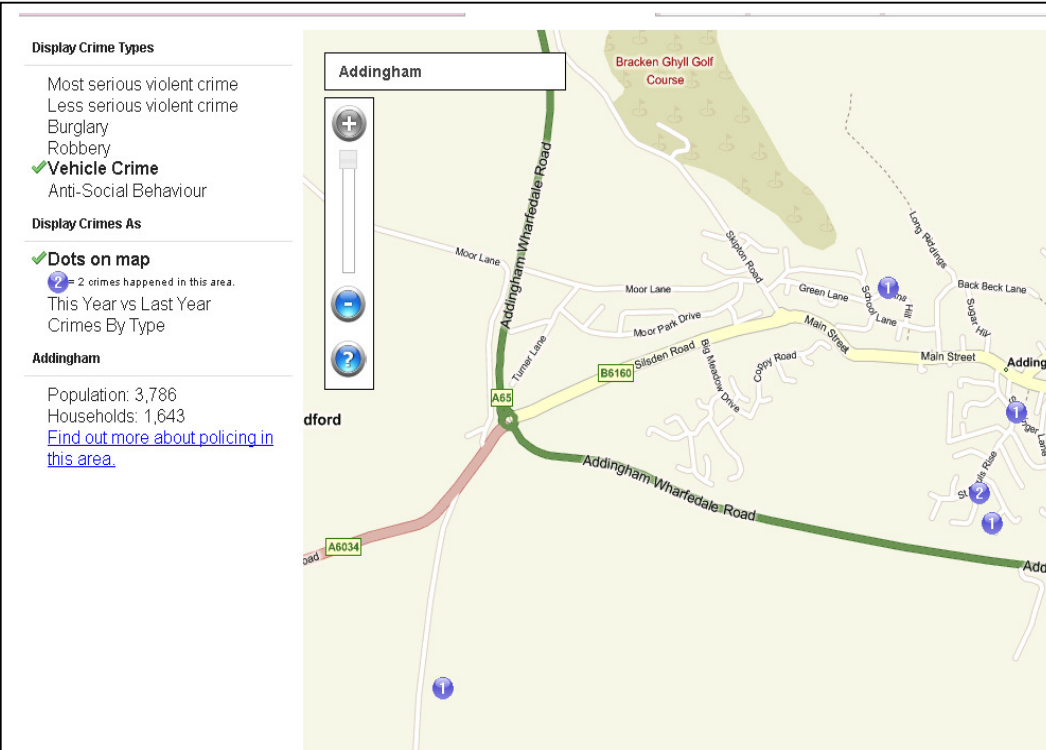
In some cases crime-mapping will give rise to public concerns, for example where the victim of a crime is concerned that his identity will be revealed or where a householder is concerned that his property has been incorrectly labelled as a crime hot-spot through the use of poor quality data or misleading mapping techniques. Publishers of crime-maps should have procedures in place to handle complaints of this sort promptly and should be prepared to amend or delete crime-mapping data where this is causing distress to

individuals. To facilitate this process, the identity of the organisation responsible for the map should be displayed prominently, with contact details for the receipt of complaints and queries about a map's content. It is good practice to offer online complaints facility. The same considerations apply in respect of other forms of data release.

Some examples of typical crime-mapping techniques.



The smallest geographical area for this crime map is division by policing district. A table gives the number of crimes, broken down by type, for the previous three months in each district. Each district contains hundreds of households.



This map uses entire postcodes to identify the location of recorded crime. Full postcodes may constitute personal data. Often, the location of the indicator at the centre of a postcode will appear to identify a specific property, particularly in rural areas. This could either identify the household where a crime was reported, or give the mistaken impression of several crimes being reported at a particular household, rather than at other locations within that postcode area.

Information Commissioner's Office

The map shows the number of recorded crimes between September 2009 and August 2010 for smaller areas (census output areas) within your neighbourhood.

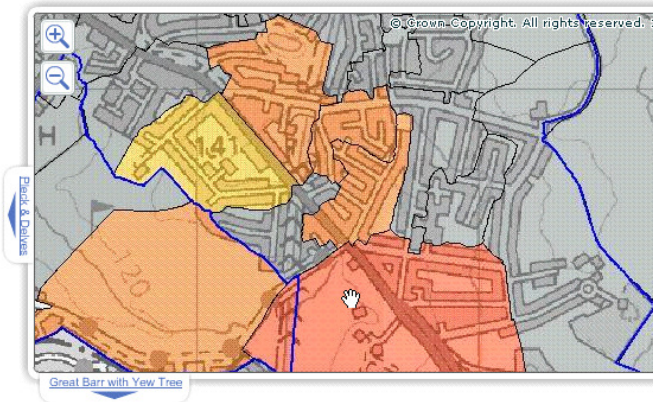
The colour coded key below shows how many crimes have occurred in each of these areas.

Crime Anti-Social Behaviour

Select the Crime types that will be shown and click the Apply button.

- Residential Burglary
- Non-Residential Burglary
- Criminal Damage
- Wounding
- Assault
- Robbery (Person)
- Theft from Person
- Robbery (Business)
- Theft of Motor Vehicle
- Theft from Motor Vehicle
- Other Crime

[Select all](#)/[Clear all](#)



Map Key

Count of Crime (Last 12 months)

- 7 to 8
- 5 to 7
- 4 to 5
- 0 to 4

Boundaries

- Neighbourhood
- Census Output Area

Points of Interest

- Police
- Fire S
- Hosp
- Neigh

[Graph View](#) [Table View](#)

This crime map goes down to the level of census output area. A census output area contains a minimum of 40 households. The map shows how many crimes of a particular type were recorded in each area.

A heat-map type approach. The advantages of this are that there is no clear link, actual or suggested, between levels and types of crime and particular locations. This avoids misleading representation, for example where all the crimes occurring in a particular area are mapped to a smaller area or specific place. Heat mapping also makes it much more difficult for the general public to establish a link between a particular crime and a particular individual.

