*All gists in the following extract have been double-underlined

The database Code of Practice April 2011 – November 2011

Should you have any queries regarding the Code of Practice or the database use in general please feel free to contact the relevant officer or any other member of the appropriate team. If you no longer require access the database please also let the relevant officer know.

Why is this Code of Practice necessary?

The database is designed to support SIS officers in meeting the Service's operational needs. It is important that in this context you can justify any the database searches you make.

We get maximum value from the database by making its contents available to all users. This requires all users to act responsibly. To do their jobs, the database users are given access to a wide range of data, which will include many individuals of no intelligence interest. For this reason searching and using bulk data are particularly sensitive activities.

We need to share and exploit the information we hold both effectively and in accordance with the law. This needs to be managed to ensure that the privacy of those whose data is within the database is respected and that data is held, accessed and disclosed only to the extent necessary for the purpose of our statutory functions.

All searches must be both necessary and proportionate and all use must comply with the legal requirements and record keeping conventions that apply to the use of the database.

Code of Practice: the database use and Standard Operating Procedures

This sets out the rules governing the use of the database. As a user you consent to comply with these rules. It is therefore important that you read and ensure that you have understood these rules. If you are unsure how these rules affect you and your work please seek advice from your line manager or countersigning officer. The provisions of these rules operate in addition to those set out in Service policy on the use of IT systems, to which you consent each time you log on to the corporate system.

Conduct and Behaviour

You are only permitted to use the database when authorised for a legitimate purpose related to the functions of your job and where you are satisfied that using the database for this purpose is necessary and proportionate. It is not possible to provide an exhaustive list of prohibited database activity, however the following activities are expressly prohibited; engaging in such activities could be unlawful and even amount to a criminal offence. They are amongst those unauthorised activities which will be regarded as a serious abuse of the system.

You must not:

Attempt to access the database by any means other than your allocated credentials.

Attempt to circumvent or defeat security measures (there may be rare exceptions to this, e.g. for staff involved in security testing, in which case they must seek prior explicit authorisation via the IT helpdesk).

Share your credentials or allow others access via your credentials.

Allow colleagues `over the shoulder' access to your use of the database.

Conduct searches on behalf of colleagues unless there is a business need for you to do so.

Use the database to search for and/or access information other than that which is necessary and proportionate for your current work. This includes searching for information about yourself, other members of staff, neighbours, friends, acquaintances, family members and public figures, unless it is necessary to do so as part of your official duties.

Share information and intelligence derived from the database in a way that is not necessary, proportionate and within the remit of the Service and appropriate to your current role and responsibilities.

Standard Operating Procedures

You must:

Comply with the database Code of Practice (including any supplementary protocols to which you may be subject), and adhere to the procedures explained during your database training. Detailed guidance on using the database is available in the database User Guide and also in the Bulk Data Policy Guide.

Ensure that your use of the database is always necessary, proportionate and relevant to your job function, ensuring that your searches are structured in a way most likely to retrieve the relevant information.

Be prepared to justify any searches you make.

Report any error in searching the database e.g. mistakenly entering the wrong name, to the security team by e-mail, explaining the circumstances.

Raise any concerns you may have about how others are using the database systems with your Line Manager or countersigning officer, you can also contact the relevant team or the security team if preferred.

Consider the propriety of sharing any database data. Results, in full detail, may be passed to BSS and GCHQ partners - this, and any resulting action, must be recorded on file [redacted]. Before passing results to other third parties (e.g police) you must seek ACTION ON from the data owners using a standard form. BSS and GCHQ will be expected to revert to SIS if they wish to use the information with other third parties (e.g police).

Additionally, Line Managers of the database users are required to ensure their staff members have signed the Code of Practice and are aware of their responsibilities under it.

Legal Context

C has a legal duty to ensure that arrangements are in place to prevent the Service from disclosing material it obtains (except so far as necessary for the proper discharge of its functions). This obligation applies equally to disclosure to persons within and outside the Service. The database may afford the potential to view information and/or data that you do not have a need to know, it is your duty and responsibility to avoid doing so as far as possible.

The Human Rights Act 1998 includes the right to privacy (article 8). Access to data on the database will involve an interference with privacy. Under article 8 this can only be justified if it is necessary for the purposes of our functions and proportionate to what we are seeking to achieve.

Logging, Monitoring and Scrutiny

The use of the database is monitored in various ways, including technically, on a continuing basis, in order to identify misuse of the system and any unusual activity that gives rise to security concerns. Users may be subject to random and routine spot checks to explain their activities on the database at any time.

Users should note that, over and above Security Department system audits, they may also be required to account for recent searches to the Intelligence Services Commissioner, as part of his regular scrutiny of the Service's work.

Breach of Secops

The Service will take action under the Service's disciplinary procedure in respect of any alleged abuses or misuse of the database, or the information and intelligence derived from it, by Service employees. This includes, but is not restricted to, those activities expressly identified under Conduct and Behaviour above. Employees should be aware that deliberate or serious abuse of the database could amount to gross misconduct and may result in dismissal. For secondees, contractors and consultants, such misconduct may result in the termination of their secondment or contract for services. In all cases, fitness to hold DV will also be examined. In addition to any internal sanctions, activity that cannot be justified by reference to our functions would be likely to be unlawful and could constitute a criminal offence.