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

The SIS database Code of Practice v3 October 2014 – November 2015

The SIS database Code of Practice

1. The database use and Standard Operating Procedures

This document 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 [redacted].

2. Why is this Code of Practice necessary?

We need to share and exploit the information we hold both effectively and in accordance with the law. The database is a powerful data exploitation tool. But its use brings some information sharing risks. These need 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 and proportionate to those aims. We get maximum value from the database by making its contents available to all users. This requires all users to act responsibly. It is extremely important that all users understand, and comply with, the legal requirements and record keeping conventions that apply to their use of the database.

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, requiring careful consideration and strict adherence by users to that which is necessary and proportionate for their work.

3. Legal Context

Data held in the database is lawfully obtained, including in accordance with the Intelligence Services Act 1994, which allows us to obtain data if it is necessary for the proper discharge of our functions. Our obligations to deal with that data lawfully do not end when we receive it. We must ensure that we handle the data within the database – including how it is accessed and disclosed - in accordance with the law.

C has a legal duty to ensure that there are arrangements 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. **Whilst the database may afford you 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.**

Section 6 of the Human Rights Act 1998 states that it is unlawful for a public authority to breach any of the rights guaranteed by the European Convention on Human Rights. These include 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**

The database must not be a 'free for all'. Users will have potential access to sensitive material. The Service's information policy and practices are designed to be compliant with the law, which dictates that users' actual access to information is limited to that which is necessary and proportionate for their work. Misuse of information, including unjustified and/or inappropriate access, would be unlawful and could in some circumstances constitute a criminal offence.

The database users are required to fill in two mandatory fields before conducting each new search, these are: Purpose and Justification. Purpose is a drop-down field with the three statutory areas of SIS' work: NS – National Security, EW – Economic Wellbeing and SC – Serious Crime. Justification is a free-text field designed for the user to provide the business need for the search, including the intelligence requirement or investigation it relates to and, where possible, a source document reference. (Advice on completing the Justification field can be found within the database.)

4. Conduct and Behaviour

You are permitted to use the database only where you have been authorised to access it 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.

You must not misuse the database or any data obtained from it. It is not possible to provide an exhaustive list of prohibited the 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 access or attempt to access the database by any means other than your allocated credentials.**
- **You must not share your credentials** with another individual or allow them 'over the shoulder' access to your use of the database.
- **You must not leave your terminal unlocked and/or unattended.**
- **You must not attempt to circumvent or defeat security measures** (there may be rare exceptions to this, eg for staff involved in security testing, in which case they must seek prior explicit authorisation via the IT helpdesk).
- **You must not use the database to search for and/or access information other than that which is necessary and proportionate for your current work.** This includes (but is not limited to) searching for information about 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. You should be prepared to justify any searches you do make.
- **You must not use the database to search on your own records** (eg. to obtain your passport number). This is to avoid unnecessary collateral

intrusion into the personal data of others. In certain circumstances, it may be acceptable to conduct a search on your own details as part of your official duties. You should not conduct such a search until you have consulted the relevant team, who will advise on the proportionality issues.

- **You must not 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.**

The database users are able to export the results of their searches into Excel and Word. However users must remain mindful that subset results from the database still represent bulk personal data. As such results should only be disseminated to colleagues that the user has satisfied have a business requirement and where it remains proportionate for them to see the information. It is most important that the database Action On process is followed for each trace derived from SIS's bulk data holdings which are to be passed beyond SIA customers.

5. Standard Operating Procedures

You have a responsibility to:

- 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 and also in the Bulk Data Policy Guide;
- Ensure that all database enquiries are necessary and proportionate for your work. Structure and target activity on the database in a way that is most likely to retrieve information that is relevant to your enquiry. If you require further guidance on searching you should seek advice from [redacted];
- Report any error in searching the database e.g. by mistakenly entering the wrong name, to a member of the appropriate 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.
- 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] to enable the relevant team to evaluate the continued retention of data. Before passing results to other third parties (e.g police) you must seek ACTION ON from data owners using a standard form (automatically copied to [redacted].)

6. 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.

7. Breach of Secops

The Service will take disciplinary action against any abuse or misuse of the database, or information and intelligence derived from it. This includes, but is not restricted to, those activities expressly identified under Conduct and Behaviour above. For staff, offences will be handled in accordance with the Service's disciplinary procedures.

Staff should be aware that deliberate or serious abuse of electronic facilities could amount to gross misconduct and may result in dismissal. For secondees, contractors and consultants, such misconduct is similarly likely to result in removal from site. In all cases, fitness to hold DV will also be examined. Furthermore, activity that cannot be justified by reference to our functions would be likely to be unlawful in article 8 terms and could in some cases even constitute a criminal offence.

8. Line Manager Responsibilities

The database needs to be used in a way that ensures the privacy of individuals whose data is within the database. Data must be held, accessed, searched and disclosed only to the extent necessary for the purposes of SIS statutory functions and proportionate to those aims.

Line Managers of the database users are required to ensure their staff members with access to the database have agreed to comply with the Code of Practice and are aware of their responsibilities set out above.

9. User Declaration

I acknowledge that I have read the database code of practice, that I understand it, and agree to abide by it.

Signature:

Date of Signature:

Staff Number:

Designation:

Name (Print):