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

The SIS database Code of Practice v3.1 November 2015 to date

The SIS database: CODE OF PRACTICE

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. If you are unsure how these rules affect you and your work please seek advice from your line manager or the relevant team. 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.

Why is this Code of Practice necessary?

The database is a powerful data exploitation tool. Exploitation of the bulk personal data held within the system has the potential to intrude into the privacy of persons, including those who are not of intelligence interest. Our use of the database must only be for the purposes of discharging our statutory functions and must be necessary and proportionate. We get maximum value from the database by making its contents available widely across the Service. This requires all users to act responsibly and in a way appropriate and sustainable for a liberal democracy. It is extremely important that all users understand and comply with the legal requirements and record keeping conventions that apply to use of the database.

Legal Context

Bulk personal 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, or otherwise in the interests of national security, for the purpose of the prevention or detection of serious crime or for the purpose of any criminal proceedings. This obligation applies equally to disclosure to persons within and outside the Service.

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 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 of the UK 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.

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 current job and where you are satisfied that using the database for this purpose is necessary and proportionate.

When you move post and your designation changes, your access will automatically be revoked. If you need access in your new role, you will need to reapply setting out in your application form why you need access and also re-sign this Code of Practice and the SecOps.

If your role changes, but not necessarily your designation, and you are required to do work that is different to the role you described in your database application form or if at any time you find that you no longer need access to the database, you must consult the relevant team.

Your Responsibilities

You must:

- Comply with the database Code of Practice (including any supplementary protocols to which you may be subject), SecOps and adhere to the procedures explained during your database training.
- Ensure that all database enquiries are necessary and proportionate for your work. You should 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 the relevant team.
- Search other corporate tools and any other sources available before you run a database search. This is so that you have gathered as much information about your subject as possible before you search in bulk personal data. You should then use as many search terms as possible in your initial database search to minimise collateral intrusion.
- Report any error in searching the database e.g. by mistakenly entering the wrong name, to a member of the security team by e-mail, explaining the circumstances

- Consider the propriety of sharing any database data. Results may be passed to MI5 and GCHQ partners. The handling instructions for such sharing must be followed. These are set out in the Data Handling tab of the database and in the export documents themselves. 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) seek ACTION ON from a senior SIS officer using the internal workflow (copied to [redacted].)
- Raise any concerns you may have about how others are using the database with your Line Manager or countersigning officer.

Misuse of information held in the database, is unlawful and could in some circumstances constitute a criminal offence. The following activities are expressly prohibited:

You must not:

- Search for 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 must be prepared to justify any searches you do make.
- Use the database to search on your own records (eg. to obtain your passport number). [Redacted]
- Seek to retrieve more information than necessary. For example, if your first search provides the required information, you should not complete a supplementary search without considering necessity and proportionality for further searching.
- 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.
- Leave your terminal unlocked and/or unattended, share your credentials with another individual or allow them 'over the shoulder' access to the database.
- Access or attempt to access the database by using another user's credentials.
- Attempt to circumvent or defeat security measures (staff involved in security testing must seek prior explicit authorisation via the relevant team in the first instance).

Logging, Monitoring and Scrutiny

The use of the database is continuously monitored to identify misuse of the system or any unusual activity that gives rise to security concerns. Users are subject to random and routine checks requiring them to explain their activities and justify individual searches.

Users should be aware that as part of his regular scrutiny of the Service's work, the Intelligence Services Commissioner picks a sample of database searches and users are required, in person, to account for their activities.

Breach of SecOps or Code of Practice

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. Offences will be handled in accordance with the Service's disciplinary procedures.

For staff, deliberate or serious abuse of SIS information holdings 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 is likely to be unlawful in article 8 terms and could also constitute a criminal offence.

Line Manager Responsibilities

Line Managers of database users are required to authorise initial applications for access to the database and ensure ongoing requirement exists. They should also ensure users agree to comply with the Code of Practice and are aware of their responsibilities as set out above.

User Declaration

I acknowledge that I have read the database Code of Practice, that I understand them, and agree to abide by them.

Signature:

Date of Signature:

Staff Number:

Designation:

Name (Print):