POLICY AND PROCEDURES ON CONFIDENTIALITY OF DATA

1. This is the statement referred to at paragraph 5.1.1 of the Bank's Statistical Code of Practice (June 2013 version), as a record of the controls in place to protect the confidentiality of information relating to individual institutions received by the Statistics and Regulatory Data Division of the Bank of England ("the Division").

2. In the normal course of events, the individual institutions with which the Division is concerned are banks and building societies undertaking business in the UK and required to report to the Bank under section 17 and/or schedule 2 of the Bank of England Act 1998 ("the 1998 Act"), supplemented by the Banking Act 2009, and regulated firms required to report to the Prudential Regulation Authority (PRA) under the Financial Services and Market Act 2000 ("FSMA"). But in some circumstances other businesses are also affected.

Background

3. The 1998 Act, FSMA and the Bank's Statistical Code of Practice require that individual institutions' reported data must remain confidential. Those data may only be revealed to third parties once certain specified criteria have been addressed. The purpose of this note is to clarify the procedures put in place to ensure confidentiality for those data, the circumstances under which disclosure can be made, and the management arrangements in place to make these procedures effective.

General security arrangements

4. All Bank staff and contractors are security cleared prior to commencing employment at the Bank. The Human Resources Directorate is responsible for ensuring that this is completed satisfactorily. If an individual needs to be issued with a security pass prior to this procedure being completed, an Executive Director's authority is required. Visitors to the Bank are required to be accompanied at all times and physical access to the Division's offices requires a staff or contractor's security pass. The Security Division is responsible for issuing passes and for the security systems within the Bank.

Specific security arrangements relating to statistical data

5. The vast majority of statistical data arrive in the Division electronically. The data have to be transmitted in a pre-specified format and encrypted, using a public key encryption system that requires each party (the reporter and the Bank) to have access to matching electronic keys to undertake encryption and decryption. These keys are stored on the Division's computer systems and access is restricted to key members of the Division's Business and Communications Group. When email communication is required, the email is encrypted during transit using Pretty Good Privacy (PGP) encryption. Reporters migrating to the new data capture system (OSCA) in 2013 will connect to the web server using HTTPS, which protects the communication channel between the reporter's system and the Bank's web server. The server itself resides within the Bank's secure extranet.

6. Individually reported data are stored on the MIDAS database (an Oracle database used by the Division to store raw data from UK banks and building societies). Access to MIDAS is controlled, so Bank staff and contractors need to be added to the group of MIDAS users on the system before they can access it. All staff in the Division have access to the data stored on MIDAS.

7. Requests for access to MIDAS from staff working in areas of the Bank outside the Division have to be cleared by a manager in the Division, and are only granted if allowing access would enable the requesting area to fulfil the Bank's functions as specified in the 1998 Act. If there is any doubt as to whether the request satisfies the legislative conditions, the matter is referred to the Bank's Legal Directorate. In practice few staff outside the Division have been granted access. A very limited number of support staff in the Bank's Information Systems and Technology Division have access to MIDAS, as most of the support is provided by the Division's own IT specialists.

8. Divisional staff often create Word documents, Excel spreadsheets or PowerPoint presentations containing confidential information. These are stored within the Bank's "Worksite" document management system. All such documents must be saved with classification 'Bank Confidential: Private - Individual Institutions Data' where the author alone has access, unless access is specifically granted to other named individuals or teams. The "Worksite" administrator periodically checks that the security classification used is appropriate. Divisional managers are responsible for ensuring that their staff have suitable training to ensure that documents have the correct classification (on any paper copies as well as the electronically stored version) and that access rights are appropriate.

<u>Regulatory data collected by the Bank on behalf of the PRA</u>

9. Regulatory data collected by the Bank from insurance companies and credit unions arrive in the Division via email and on paper returns. Paper returns are scanned into the Bank's "Worksite" document management system with the classification 'Bank Confidential: Private - Individual Institutions Data' and access granted to named individuals and teams (similarly to paragraph 8 above). Credit Unions' data are loaded into the BSD database. Access to this database is limited to those who need it for business reasons.

10. Regulatory data that do not form part of the PRA Handbook are collected via email using PGP encryption (as detailed above). These data are loaded into the FMS database and are also used in a number of database systems. Access to these databases is limited to those who need it for business reasons.

Regulatory data collected by the Financial Conduct Authority (FCA) and provided to the Bank
11. Regulatory data detailed in the PRA Handbook are reported electronically to the FCA by banks and building societies. These returns are loaded into the FCA's GABRIEL data collection system. Bank staff may be granted access to GABRIEL, but this is limited to those who have a business need. The data are transferred to the FCA's COGNOS data analysis system to which Bank staff can also be granted access if they have a business need.

Release of confidential data to specific third parties

12. The 1998 Act permits the disclosure of confidential information by the Bank to enable or assist it to discharge specific functions, particularly as a monetary authority, and to specified third parties to allow them to fulfil certain functions, specified in paragraph 3 of schedule 7 to the 1998 Act. The scope of permitted disclosure has been enlarged by the Banking Act 2009.

13. The legal framework for the sharing of data is included in the introductory notes to the Reporting Definitions, available on the Bank's website.

14. Individual statistical data reported by banks and building societies may be transferred to the Prudential Regulation Authority (PRA) or the Financial Conduct Authority (FCA), to assist them with the discharge of their functions under FSMA and other legislation. Banks and building societies will be informed when they join the population of reporting institutions that the statistical data they report will be routinely shared with the PRA and the FCA.

15. Under the same provision of the 1998 Act, the Bank may also share confidential information with the Office for National Statistics (ONS) under a delegation from the Chancellor of the Exchequer, to assist in discharging its responsibilities under the Statistics of Trade Act 1947. More rarely, information may also be shared with the Treasury to enable or assist it to discharge functions under FSMA.

16. There is a limited number of other named institutions with specific functions to whom disclosure is also permitted. The table that lists them is reproduced on page 49 of the Bank's Code.

17. In addition to the identified institutions, the Bank is generally empowered to disclose information for the purpose of enabling or assisting it to discharge its functions as a monetary authority, supervisor of funds transfer systems, or for cash ratio deposit purposes, under paragraph 2 of schedule 7 to the 1998 Act. This may include disclosure of selected information to the Bank for International Settlements, European Central Bank, European Systemic Risk Board or International Monetary Fund, for example.

18. Under section 246 of the Banking Act 2009, the Bank may disclose any information that it thinks is relevant to the financial stability of either individual financial institutions or one or more aspects of the financial systems of the UK to the Treasury, the PRA, the FCA, the Financial Services Compensation Scheme, an authority in a country outside the UK exercising similar financial stability functions, and the European Central Bank.

19. The Bank may receive confidential information from the PRA or the FCA through one of the 'gateways' detailed in the Financial Services and Markets Act 2000 (Disclosure of Confidential Information) Regulations 2001 (the "Confidential Information Regulations") as amended. If the information is "single market information", then the Bank may only disclose that information to third parties to enable or assist it to discharge its functions either as a monetary authority or in relation to overseeing payment systems and clearing and settlement systems. If the

confidential information the Bank has received from the PRA or FCA is not "single market information", then it may disclose it to third party recipients detailed in the Schedules to the Confidential Information Regulations for the functions of those recipients listed in the Schedules.

20. The Freedom of Information Act 2000 provides a number of exclusions under which data need not be released to third party enquirers. Any information held by the Bank with respect to its excluded functions under that Act may be withheld. These are defined as (a) monetary policy, (b) financial operations intended to support financial institutions for the purposes of maintaining stability and (c) the provision of private banking services and related services. Other exemptions may also apply and, if there is any doubt, staff are required to consult their manager and/or the local Freedom of Information representative.

21. Permitted external disclosures are always to be cleared by a Divisional Manager, with the confidential nature of the information and restrictions on its use and onward disclosure being emphasised.

Release of aggregate or publicly available data to unspecified third parties

22. Disclosure of data is not restricted if framed in such a way that data relating to a particular person cannot be deduced from it; nor if the data have already been made available to the public from other sources. This means that most aggregates can be published, as they normally include data relating to many banks and building societies. From time to time it is helpful to users to annotate an aggregate with an appropriate note about a specific transaction, even if that transaction has already been reported in the press. If the note referred to or might reveal a particular bank or counterparty, we would inform that party in advance as a matter of courtesy. If the note revealed information that was not already in the public domain, the precise wording would be agreed with the appropriate parties who would have the right to refuse to grant consent to publish the reference. Even where the reference is not by name, it is still cleared with the relevant parties. All statistical press releases are cleared by a Divisional manager: it is his or her responsibility to ensure that all the necessary parties have been contacted and appropriate permissions obtained.

Fewer than three reporters

23. From time to time, an aggregated series will include only one or two institutions' data, such that an individual institution's data could be deduced from it. All statistical aggregates are run through the automated checking system within MIDAS, which highlights any series that have fewer than three contributors. Institutions that are either sole or dual reporters are contacted to establish whether or not they will allow publication. If permission is given, this is recorded. This may include a mandate to continue to publish in future months, or a request that the institution is contacted on each occasion. If permission is not given, the data are suppressed (shown on publications as two dots) and another related series may also have to be suppressed if publication allows the suppressed series to be deduced. For example, if series A plus series B equals a total shown as series C, and series A has to be suppressed, then either series B or series C must also be suppressed.

24. As above, the responsibility for ensuring these procedures have been followed rests with the manager of each team within the Division responsible for creating the published outputs.

Statistics and Regulatory Data Division

July 2013