Bank of England Information Security Classification Scheme – External users

If Bank of England information is legitimately shared with you, it is important that you know how to handle it to keep it secure while it is being viewed, circulated and disposed of. You must handle Bank of England information with due care, and where applicable, in line with statutory obligations, such as data protection legislation.

The Bank of England Information Security Classification Scheme has three classifications – OFFICIAL, SECRET and TOP SECRET . The OFFICIAL tier is divided into four handling caveats, - BLUE, GREEN, AMBER and RED.

The below table summarises the handling requirements for OFFICIAL information. These requirements apply whether the information was shared with you verbally, electronically, in paper format, or in any other way.

Classification	Definition	Handling Requirements
OFFICIAL-BLUE	Information that is in the public domain or has been cleared for publication.	Information can be discussed and shared without restrictions whether verbally, in paper or in electronic form.
OFFICIAL-GREEN	The Bank's routine information, suitable for justified general distribution internally. When shared externally there must be a business justification and permission from the owner.	Information needs to be stored securely and appropriate technical controls applied to ensure the access is restricted to those who have a valid business justification to receive it. Permission should be sought from the Bank before sharing onwards. You should consider your surroundings before viewing (either in paper or electronic form) or verbally discussing the information to avoid being overlooked or overheard. Information in paper format must not be left unattended and must be destroyed in a secure way such as shredding.
OFFICIAL-AMBER	The Bank's more sensitive routine information. The information may be market sensitive and/or include personal data or may be confidential and/or subject to legal professional privilege. Access must be restricted internally and when shared externally, there must be a business justification, permission from the owner and a clear 'need to know' for the recipient.	Information must be stored securely and appropriate technical controls applied to restrict access to those with a clear need to know it. Permission must be sought from the Bank before sharing onwards. Electronic information must be encrypted in transit. You must not view the information (either in paper or electronic form) where it can be overseen. You must not discuss the information where you may be overheard. Information in paper format must not be left unattended and must be destroyed in a secure way such as shredding. For more information about why and how the Bank of England handles personal data, please see the Bank of England's privacy notice (https://www.bankofengland.co.uk/legal/privacy).
OFFICIAL-RED	The Bank's most sensitive routine information which is shared with named individuals only, managed via an insider list. The information may be market sensitive and/or include personal data or may be confidential and/or subject to legal professional privilege.	Information must be stored securely and appropriate technical controls applied to restrict access only to the named individual receiving it. Information must not be shared with anyone other than the named recipient. Electronic information must be encrypted in transit. You must only view and discuss this information in a secure location. Information must not be printed out. For more information about why and how the Bank of England handles personal data, please see the Bank of England's privacy notice (https://www.bankofengland.co.uk/legal/privacy).

Anyone needing to receive information from the Bank of England classified as SECRET or TOP SECRET will be individually briefed in advance on the necessary security arrangements and handling requirements.

OFFICIAL-BLUE