BANK OF ENGLAND

Our Code

What matters most

September 2018

Dear colleagues

The Bank's mission is to promote the good of the people of the United Kingdom through maintaining monetary and financial stability. Our ability to achieve that mission relies on our living to the highest standards of integrity and thereby maintaining public trust.

Our Code encompasses our conflicts of interest policies. It also highlights, brings together and provides context for certain other key policies.

The values and principles embodied in Our Code are not new. They are based on core principles derived from the values we established together in our Strategic Plan, reiterated in Vision 2020, and the Nolan Principles of public life. They embody the leadership expected of us and they are in accordance with the principles we expect of senior managers in the firms that we regulate.

Integrity is a core principle of Our Code. Adhering to Our Code is not simply about observing the letter of the requirements and the policies referred to in it; they cannot provide for every contingency. We aspire to set an example of the best in public service: complying with Our Code is about understanding and embracing the principles and spirit behind it.

Our Code is clear about the disclosure and approval requirements under the policies and is focussed on what matters most. All such key requirements are included on the face of Our Code, where appropriate, making it easier for colleagues to follow and to ensure adherence. Our Code this year also reflects the changes to Data Protection law and the additional steps we must all take to protect the information we hold.

We encourage your voice to be heard: speaking up and reporting on matters of concern, as set out in Our Code.

The Bank is a better place where we encourage errors to be redressed, not hidden; where we take prompt responsibility; and where we demonstrate that colleagues have nothing to fear from admitting an honest mistake. The Bank does not operate a 'one strike and you're out' policy for such matters.

Our Code applies to all of us: Governors, members of the Financial Policy Committee, Monetary Policy Committee and Prudential Regulation Committee and colleagues from across the full range of the business. The non-executive directors are subject to a separate 'Court Code' which, insofar as is relevant to their functions, is consistent with Our Code.

The Governors

Contents

Introduction to Our Code

Our Code represents our commitment to how we work at the Bank and how we should conduct ourselves – both within and outside the Bank.

Our Code sets out our principles of staff conduct, policies and supporting requirements: showing behaviours that our colleagues, counterparties and the public should expect from us. It is publicly available.

Our Code is in four sections.

Acting with integrity and demonstrating impartiality…

brings together the Bank's conflicts of interest policies, setting out our disclosure and approval requirements, and includes the proper use of Bank resources. These requirements apply to all of us at all times. We are individually responsible for making full, timely and accurate disclosures. This enables others within the Bank to decide whether these disclosures could represent a conflict of interest, and how any such conflicts should be handled.

Being open and accountable…

focuses on policies about how we communicate. We have made Our Code clearer about our record keeping requirements and how we engage openly with the public and stakeholders. This section also includes policies on sharing information internally, disclosing information outside the Bank and escalating external misconduct concerns.

Being safe and secure…

covers some of the fundamentals of how we work, at a time of heightened physical and cyber-security. As a policy-making institution and supervisor, we handle a very considerable amount of sensitive information. Mishandling that information could cause reputational harm to the Bank and undermine our ability to fulfil our mission. Also, as a financial institution, we must remain vigilant to the risk of financial crime.

Creating an inclusive and empowering culture…

reflects the Bank's commitment to wellbeing, diversity and inclusion and confirms we do not tolerate discrimination, bullying or harassment. It includes details of how we are empowered, without any fear of retaliation, to 'speak up' about malpractice or misconduct, or raise serious concerns if we feel the Bank or anyone in it is contravening the policies in Our Code.

Attestation

You are expected to attest to Our Code annually, confirming that you have read, understood and complied (as appropriate) with policies in Our Code. This is an opportunity for each of us to check that we are up to date with the disclosures which should be made throughout the year and approvals which should be sought.

Compliance and breaches

You are expected to protect yourself, colleagues and the Bank by identifying and reporting conduct breaches promptly. If you are aware of a conduct breach, you should inform your manager, making any relevant declaration with full details as quickly and as completely as possible.

As the Governor has said, mistakes sometimes happen. Credit is given for prompt and full reporting. While failure to comply with Our Code and its associated policies could lead to disciplinary action, many conduct breaches are minor and/or a 'one-off' lapse of attention or judgement. In such cases, an informal response is often sufficient.

Managers should ensure they understand their responsibilities to deal with such matters promptly; and report as an 'incident' and/or report to the Compliance Division under the >**Guidance on managing breaches of Our Code and related policies**.

Page 27-29 of Our Code includes useful information on: 'What do I need to disclose or seek approval/permission for?', 'How can I raise or report matters of concern?' and 'Who do I speak to for further information about the policies?'.

Our Code represents our commitment to how we work at the Bank of England.

You are required to:

Know, understand, and comply with Our Code and ask questions if you need clarification or advice

Gain permissions or make the disclosures required

Confirm annually that you have read, understood and complied (as appropriate) with policies in Our Code

Report breaches, and challenge where you have concerns; escalate to your management if you feel you need to, or, where appropriate, use the Bank's Speak up policy.

Acting with integrity, demonstrating impartiality

Integrity is one of the principles of public life. Our personal interests should never influence our decisions at work. We must be free of any suggestion of inappropriate influence. Selflessness, objectivity and impartiality are a core part of our Bank values.

We strive to be objective in our decision-making and decisive in our actions. We take pride in the quality and the impartiality of our analysis and research. We engage with others professionally and make decisions fairly and on merit, using the best evidence available. We know that our reputation for impartiality and independence is vital to our effectiveness and, if lost, would be hard to recover.

The Secretary of the Bank – as the Bank's 'Conflicts Officer' – has senior manager responsibility for promoting the importance of identifying and managing conflicts of interest throughout the Bank.

Principles

We must all follow these key principles:

- We must be open about relationships and personal interests that might be seen as influencing our independence of judgement.
- We must not seek to make a profit (or avoid a loss) for ourselves or for others by making personal use of information acquired in the course of our duties at the Bank. We must use Bank resources responsibly for the public good.
- We should exercise caution in the management of our finances and not undertake transactions that might embarrass the Bank or harm its reputation.
- Our Declaration of secrecy requires us to maintain the strictest secrecy over information that we acquire while working at the Bank (see page 22).
- Like other colleagues in the public sector, we must be seen to be apolitical and must not allow our decisions to be, or appear to be, inappropriately influenced.
- We are individually responsible for making full, timely and accurate disclosures and seeking all the necessary approvals required by Our Code. This enables others within the Bank to decide whether these disclosures could represent a conflict of interest, and how any such conflicts should be handled.

General requirements

We are expected not to allow outside interests to influence or be suspected of influencing our judgement or decisions in our work at the Bank. We need to ensure that actual or perceived conflicts of interest, and perceptions of influence or unfair advantage, do not arise between the work of the Bank and our personal lives – whether from close personal relationships, business relationships, outside activities or from the nature or timing of our personal financial transactions. Policies in this section of Our Code contain disclosure and approval requirements, to safeguard ourselves and the Bank.

In addition to any disclosure and approval requirements set out in this section, you should inform your line management if you consider there is a risk of an actual or perceived conflict of interest, or a perception of influence or unfair advantage. You will need to help mitigate or resolve any such issue. It is particularly important to inform your new line manager of these when you change roles or teams within the Bank.

When incurring costs on behalf of the Bank, for example expenses or travel, you must ensure that these are reasonably incurred for the public good, in accordance with the Bank's policies.

If you are joining the Bank, the disclosure and approval requirements apply to existing roles you hold (directorships; relevant community or charity roles; other employment or certain political activities) and you will need to seek approval immediately to determine whether you can retain those roles.

If you are a Head of Division (HoD) or more senior, references in these requirements to your 'HoD' should be read as referring to your line manager.

The Bank will be introducing a new electronic disclosure and approvals system in 2019, replacing the systems referred to in this section.

Where Our Code sets a specific process for disclosures or approvals, the Secretary of the Bank ('the Secretary') may specify alternative processes in particular cases.

On appointment and annually as part of attestation, Governors and Policy Committee members will have a face-to-face meeting with the Secretary to provide an opportunity for full review of the individual's existing declared interests and to allow individuals to obtain advice about what needs to be disclosed.

Our personal interests should never influence our decisions at work, and we must be free of any suggestion of inappropriate influence.

Personal relationships

We are required to disclose certain close personal relationships within the Bank or externally that could create or be perceived as creating a conflict of interest, influence or unfair advantage.

This is particularly important in areas where there is dual control of assets or signature panels for release of payments. Also, you should not directly supervise, negotiate with, approve or otherwise participate in hiring, compensating, promoting, or retaining any person with whom you have a close personal relationship.

Beyond this, if you know someone seeking employment with or business from the Bank you should discuss it with your line manager before you become involved in any way with the related decision-making process.

Sometimes, a close personal relationship may give rise to an actual or perceived conflict of interest.

You must disclose in HRConnect and **notify** your line manager of each of the following **>close personal relationships** and update if there are any changes regarding:

- any close family members (ie spouse/partner, parents, siblings, children):
  - working in the Bank;
  - working in financial, economic or political journalism;
  - working in a Bank-regulated firm;
  - working in a significant dealing counterparty of the Bank;
  - working in a firm holding or tendering for a contract with the Bank;
  - holding a national elected public office (MPs, the Scottish Parliament, the London, Northern Ireland or Welsh Assemblies).

- any other close personal relationship with an individual, or an organisation, that could reasonably give rise to an (actual or perceived) conflict of interest in relation to:
  - a specific decision in which you are involved; or
  - your work more generally, given your role and that of the individual or organisation in question. Such conflicts relating to a particular situation are likely to arise only rarely.

If you are unsure about whether to disclose such a relationship, please seek guidance from the Secretary's Department before making a declaration.

Please also seek guidance if you need to make lengthy inquiries to judge if you need to disclose a family relationship. Where an individual could not reasonably be expected to be aware of a relative's personal situation, the Secretary's Department may allow an exception to the disclosure requirement.

Discussions on prospective employment with Bank regulated firms or Bank suppliers

Actual or potential conflicts of interest may sometimes arise where we are in discussion with a prospective new employer with whom we engage on work-related matters. HR can help determine whether your line manager needs to be alerted in order to mitigate any such risks.

You are encouraged to make the HR Employee Relations Team aware promptly of any active two-way discussions about prospective employment that you are having with any organisation that is regulated by the Bank or that you have contact with as a Bank supplier.

If you are Scale C and above, you **must notify the Secretary** of any such discussions, and take advice on the management of any conflicts that may arise. The Secretary will maintain the confidentiality of the information you provide, unless the nature of the conflict(s) identified make some form of disclosure to management unavoidable. That would be discussed fully with you in advance.

Personal financial matters

Our own savings, investments and borrowings sometimes give us a personal interest in decisions that are to be made by the Bank; and it is important to show that our own decisions about investments are not influenced by information that we know only as a result of working here, which is often not in the public domain.

Furthermore, insider dealing (trading on the basis of 'insider information' or disclosing it to someone else so they can benefit) is a criminal offence, likewise the manipulation of markets – such as spreading false rumours.

To safeguard ourselves and the Bank, we must disclose certain financial relationships. We must seek prior approval for certain personal financial transactions that we wish to make, and avoid some transactions altogether.

The financial relationship and personal financial transaction requirements apply to:

– your own financial relationships and transactions; and

– any financial relationships or transactions for another individual or organisation that you direct or advise on, including where acting as an executor of a will, trustee, director or shareholder.

Financial relationships

You must disclose in HRConnect each of the following **>financial relationships**, and update if such financial relationships change:

Direct holdings of securities or related investments in a Bank-regulated firm, or its financial holding company, including stock options and share related reward schemes.

A balance or deposit in a Bank-regulated firm of a value greater than the current compensation limit set by the Financial Services Compensation Scheme (currently £85k per person per firm).

Holding an investment or pension product with a Bank-regulated insurer whose return depends in part on the profits of the insurance company – for example a 'with-profits' policy.

Any other financial relationship if it could reasonably be considered to be a potential conflict of interest. This would include deferred remuneration arrangements.

If you are unsure about whether to disclose such a financial relationship, please seek guidance from the Secretary's Department before making a declaration.

To ensure that our integrity is protected, we must disclose certain financial relationships.

Personal financial transactions

The approval requirements for certain personal financial transactions are designed to protect you and the Bank from potential reputational harm. You must not carry out the transaction before approval is granted or if approval has been refused.

You must obtain advance approval via HRConnect giving at least one working day's notice for these **>personal financial transactions**:

Arranging a mortgage on a property, whether the property is for your own use or for investment purposes.

'Arranging' in this context means entering into a new or revised agreement to borrow, or an agreement in principle, on stated terms and conditions.

Dealings in exchange-listed securities and related investments, dealings in collective investment schemes (eg unit and investment trusts) **and commodities such as precious metals** (eg gold).

Transactions through crowdfunding and peer-to-peer lending platforms are covered where they are substantially the same as an investment, rather than a donation. You do not need to seek approval for dealings in investments in the core funds permitted within the Bank's Supplementary Pension Plan, or funds of a similar composition offered by alternative providers.

Setting up or transferring a personal pension plan, and taking or approving decisions relating to the investments within such a plan.

Switching between core funds within the Bank's Supplementary Pension Plan, or funds of a similar composition offered by alternative providers, does not require approval.

Transferring more than £5,000 from a bank where you hold a balance greater than the FSCS limit (currently £85K per person per firm) to another institution (including National Savings and Investments).

You should not split up financial transactions in order to circumvent this requirement.

Transactions in foreign exchange that seek to hedge or take a position.

You do not need approval for transactions in foreign exchange relating to the purchase of goods or services, or to an investment that has been separately approved under this policy.

Carrying out any other financial transaction that could reasonably be seen to be sensitive.

This would include, for example, withdrawing deposits from a firm where you know of contingency planning being carried out, or are aware of adverse stress testing results or a breach of regulatory requirements, or where you are involved in any intervention by the Bank with respect to that firm.

If you are unsure about whether to seek approval for a personal financial transaction, please seek guidance from the Secretary's Department.

Some personal transactions, such as mortgages, take some time to complete after approval; please execute any approved transaction promptly and consider seeking re-approval where there has been a material delay between the initial approval and the transaction.

Personal portfolio managers and discretionary portfolios

The personal financial transaction approval requirements do not apply to investment assets where they are managed by a personal portfolio manager with full discretion over investment decisions, on terms that have been approved by the Secretary. If you are selecting specific investments/ investment funds you must review the table on page 9 to check whether your transactions need advance approval.

Additional requirements and guidance for Governors, Executive Directors and members of Policy Committees etc.

If you are a Governor, Executive Director or a member of the MPC, FPC, PRC or some other Bank committees (eg FMI Board, SONIA Oversight Committee, RTGS/CHAPS Board), you must provide an annual paper-based report to the Secretary of your stock of financial assets and liabilities.

It is highly undesirable for members of this group to be actively involved in managing an investment portfolio, even within the transaction approval arrangements. Accordingly, if you hold a substantial portfolio you are strongly advised to place it under full discretionary management on terms approved in advance by the Secretary.

Prohibited transactions

Certain kinds of transaction are never allowed.

Do not acquire or actively manage marketable debt or equity interests (eg bonds or shares) in any Bank-regulated firms, or their financial holding companies.

If you join the Bank with holdings of such securities you will be able to retain them, exercise rights arising from them or sell them, but you may not acquire more or actively manage them. You must declare your holdings as 'financial relationships'. If you exercise your rights in relation to your prior holding or sell these securities, you should obtain pre-approval as a personal financial transaction.

Do not undertake transactions whose main purpose is speculative (eg transactions motivated by a desire to make quick capital gains) including in cryptocurrencies.

Do not bet on financial variables or indices.

Do not take out a contract for differences (which includes spread-betting) in relation to securities, the UK equity market, UK indices/sectors or economic variables of direct interest to the Bank and its forecasting processes (eg commodity or currency markets).

Do not invest in collective investment schemes that are unduly weighted towards investments in the financial services industry. A balanced portfolio may contain some financial services securities.

Certain kinds of transaction are never allowed.

Roles and activities outside the Bank

Directorships

Permission will not normally be granted for you to become a director of a company running a business. This can give rise to a range of financial, legal and reputational risks. It will not be granted in the case of organisations engaged in financial markets or Bank-regulated firms or their holding companies. Directorships of non-trading companies – for example, those set up by leaseholders in a block of flats to acquire or manage the freehold – and social enterprises or charities raise fewer concerns. If you wish to become a director of a company (whether non-executive or otherwise), approval is required in advance. Any real or perceived conflicts of interest will need to be discussed and resolved.

You must seek approval via HRConnect before becoming a **>director**.

Your request will be considered by the Secretary's Department and your HoD.

If you are a director through your employment at the Bank (eg of a Bank subsidiary) this should also be disclosed in HRConnect, so that a central list is maintained. Examples include directors of the Bank of England Asset Purchase Facility Fund Limited and director trustees of BE Pension Fund Trustees Limited.

Community and charity roles

The Bank encourages employees to take on roles with charities and community organisations in a personal capacity. Certain roles also have formal duties, for example as charity trustee or school governor. Although usually uncontentious, these may occasionally be controversial – as public cases have shown. Disclosure requirements apply to these kinds of roles so that we can consider, mitigate or resolve any real or perceived conflicts of interest or reputational concerns. If these exist, we will discuss how they may be handled with you. In rare circumstances you maybe asked to stand down from the role.

You must disclose via HRConnect before taking on a **>charity or community role** with formal responsibilities such as:

– a charity trustee or member of a charity's investment committee;

– a school governor.

Your disclosure will be reviewed by the Secretary's Department and your line manager/HoD.

If the nature of the charity/organisation and its activities changes, you should notify the Secretary's Department and your line manager/HoD.

Please note that if you make or advise on financial decisions as part of such a role then the 'personal financial transactions' pre-approval requirements will apply, as though the transactions were your own.

You do not need to disclose other forms of community and charity volunteering, such as coaching a football team, being a guide leader, helping with a charity event or working in a charity shop, but you will need to discuss this with your line management if it could have an impact on your work at the Bank, eg due to time-commitments.

Any compensation you receive for community or charity roles or volunteering (other than expenses) should be refused or donated to charity, rather than being retained, unless the role has been approved as 'other employment' – see page 12.

Some charities take the form of companies, in which case the approval procedure in the 'Directorships' policy applies.

We know that our reputation for impartiality and independence is vital to our effectiveness, and, if lost, would be hard to recover.

Other employment

Most people at the Bank do not have other employment. You will need to seek the approval of your HoD before you take up additional employment. This is in case it may give rise to an actual or perceived conflict of interest, influence or undue advantage and/or reputational harm to the Bank or otherwise be considered detrimental to the Bank's interests. Your HoD will also need to consider whether this might impact on your ability to deliver your work at the Bank to the necessary standard. Sometimes, an external role might bring benefits; for example, a research career at the Bank might involve occasional teaching assignments or guest lecturing as part of maintaining an academic network.

You must seek approval from your HoD before taking on **>other employment**.

Please save evidence of the approval in your staff folder in Filesite.

Some external roles are never permitted as they inherently give rise to the risk of a conflict of interest.

Roles which are never permitted

Some roles are never permitted as they inherently give rise to the risk of a conflict of interest or perception of advantage.

Do not in any circumstances:

- act as a dealer in gold or foreign exchange, whether as a principal or intermediary;
- act either directly or indirectly as a broker or dealer or other intermediary in buying, selling or exchanging any securities on commission;
- receive any commission or gratuity from such a broker or dealer for recommending business to them.

Personal data and changes of personal circumstances

The Bank needs to have your up-to-date personal details and information about certain personal circumstances.

You must complete personal data reviews when prompted and keep your personal data in HRConnect up to date.

You must complete Security Vetting forms when requested.

You must disclose to the Security Vetting team details of **>changes in personal circumstances** that may affect security clearance, including:

- a change in partner, getting married or entering a civil partnership;
- a change in nationality;
- receiving a county court judgement;
- receiving a police caution, being charged with a criminal offence or conviction; and
- a material adverse change in personal or financial circumstances.[1]

1 The Bank offers a range of services to support colleagues' physical and mental wellbeing, including for colleagues facing financial difficulty.

Political activities

We recognise that, in engaging with your community, you may want to engage in political activities. The following requirements reflect that the Bank is apolitical. The requirement to obtain consent if you wish to stand for local or national elected office is in place because the Bank will wish to consider any sensitivity arising from your work, and any risk to our reputation for impartiality.

If you engage in any **>political activity**:

- Make clear that your involvement is solely in a personal capacity.
- Do not publicise that you work for the Bank.
- Take care to avoid any suggestion that the Bank supports or endorses your activities.
- Do not engage in political activity while on duty, or using Bank premises, systems or resources.

You must seek consent from the Secretary via HRConnect, giving at least three months' notice, if you wish to stand for local or national elected office. In exceptional circumstances, the Secretary may allow a shorter notice period.

The Secretary may consult local management and Governors.

You must notify the Secretary via HRConnect if your political activity is likely to include involvement in party organisation, fundraising or campaigning (eg door-to-door canvassing).

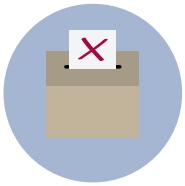
You do not need to notify the Secretary about providing administrative support, such as delivering leaflets.

If you decide to stand for national elected office, you will be required to take unpaid leave from the point of adoption as a prospective candidate until the election. If you are elected, you must resign immediately.

In principle, the Bank is prepared to allow a member of staff elected as a member of a local authority or similar body to remain employed by the Bank.

'National elected office' includes: Member of Parliament; Scottish Parliament; or the London, Northern Ireland or Welsh Assemblies; or any other remunerated elected office.

We must be seen to be apolitical and must never allow ourselves to become open to the perception that our decisions have been inappropriately influenced.



Entertainment and gifts

Our role as the United Kingdom's central bank requires many of us to develop contacts with external parties. This will often involve the giving and receiving of hospitality. Occasionally we may be offered gifts. The Bank's position as a public body means that it has to apply, and be seen to be applying, high standards of ethical behaviour to maintain objectivity and commercial impartiality and to protect against any suggestion of impropriety.

We apply high standards of ethical behaviour to maintain objectivity and commercial impartiality.

When following the rules below, we need to apply common sense about whether an offer of entertainment or a gift should be accepted, and should consider the accumulating effect of entertainment and gifts on individuals or areas. If the acceptance of entertainment or gifts by an individual member of staff was challenged, it would be necessary to show that acceptance was lawful, appropriate, consistent with the Bank's rules, and did not give concern that personal judgement or integrity had been compromised.

UK legislation on bribery applies to us all at the Bank. Under the Bribery Act 2010, it is an offence for a Bank employee to offer, promise or give a bribe to another person, or to request, agree to receive or accept a bribe from another person, and individuals may be subject to prosecution. The Bank may also be found liable if it fails to prevent a bribe by an associated person.

General requirements

Do not accept any fee, gratuity, gift, hospitality or entertainment of any kind in your official capacity without authority from your Manager/HoD.

Do not offer any fee, gratuity, gift, hospitality or entertainment of any kind in your official capacity without authority from your Manager/HoD.

Do not solicit gifts from a Bank supplier for yourself or for any other purpose (this includes soliciting prizes for charity events).

If you are in any doubt about accepting or offering a gift or entertainment, then you should discuss this with senior management before doing so.

Where necessary, business areas may, with the approval of the Secretary, adopt additional local business area rules for gifts and entertainment to suit the particular circumstances of their work. These must be at least as stringent as the Bank-wide rules. As different areas may have different general permissions in place, you should make sure you understand any general permissions in your area.

Entertainment rules

Offers of entertainment may be accepted, or made, where they are necessary to develop and maintain outside contacts relevant to work responsibilities. They should be restricted to working lunches or similar events as far as possible.

Light refreshments at a meeting, such as tea, coffee and biscuits do not fall under these rules.

Please decline any offer of entertainment if it is, or might be perceived as:

- excessive;
- putting you or the Bank under an obligation;
- offered to influence any decision of the Bank;
- liable to bring you or the Bank into disrepute.

'Excessive' includes offers of entertainment that are disproportionately lavish (such as invitations to expensive or exclusive cultural or sporting events), over-frequent (including an inappropriate number of invitations from a counterparty or supplier to individuals or team-members at the Bank), or too time-consuming.

Please decline any invitations from firms regulated by the Bank or the FCA without the prior approval of an Executive Director or a Governor (which may be a general permission rather than case by case).

For example, it would not be appropriate to accept hospitality from professional advisers or suppliers which was, or could be perceived as, seeking to influence a decision to use their services or procure goods.

Business contacts may also be personal friends. For the purpose of these rules, any hospitality enjoyed in your role at work should be reported unless it is both clearly offered and accepted in a personal capacity, not an official capacity. Relevant factors which may help show that the hospitality is offered and accepted in a personal capacity include whether a firm or an individual is paying for the hospitality.

If you are invited to an event accompanying your spouse or partner, you should treat the invitation as though it was to yourself at the Bank and apply these rules accordingly.

If in doubt about whether it is appropriate to accept an invitation, please discuss with senior management or seek advice from the Secretary's Department before accepting the entertainment.

Entertainment should be restricted to working lunches or similar events as far as possible.

Gift rules

Please discourage the presentation of gifts as far as possible.

However, where refusal would cause offence or embarrassment, and the value is modest, you may accept a gift.

You must not accept:

– cash or retail vouchers (except for commemorative coins/specimen notes);

– electronic devices (for security reasons).

You may keep a gift up to the value of:

– £30, if your HoD gives permission;

– £100, if the Secretary gives permission.

Sometimes gifts take the form of 'prizes' offered by a corporate entity when you are on Bank business. The same rules apply.

If you have accepted a gift and you are not given permission to keep it:

– pass it to Community for disposal for charity;

– give it to charity directly if the value is under £30;

– if it has a value less than £100 it may be disposed of for charity under local arrangements (eg raffle) approved by your HoD; or

– if the item is perishable, dispose of it as instructed by your HoD if the value is less than £30, otherwise, seek guidance from the Secretary's Department.

Entertainment and gifts must be fully and accurately recorded for reporting in accordance with arrangements approved by the Secretary's Department. This includes recording gifts you have accepted, that you are subsequently not given permission to keep. This process is subject to audit.

Please discourage the presentation of gifts as far as possible.

Being open and accountable

We want to be open and accountable to each other, to Parliament and to the people of the United Kingdom. Our decisions and actions are subject to public scrutiny.

We must communicate effectively across the Bank, the public sector and the financial sector and with the public. In our communications, we are open, honest and straightforward. This is supported by the policies in this section and by good record keeping. When sharing information in the Bank and making information available outside the Bank we need to be mindful of the obligations set out in the policies in this section, and the circumstances in which we have a duty to escalate – including misconduct concerns.

Good record keeping is vital. Records represent our institutional memory and allow for proper debate and questioning.

Record keeping

Good record keeping is vital. In the course of our work, we make critical policy, supervisory and operational decisions that have a broad impact. We are ultimately accountable to the people of the United Kingdom for those decisions. We are responsible for the information entrusted to us in the work we do and we have to be accountable for managing it with due care, skill and diligence.

It is key therefore to maintain our records properly and securely.

The >**Records Management Policy** sets out an overall framework for achieving this. Ensure you are familiar with this.

Key requirements are:

- Keep accurate and complete records of your business activities, in particular notes for record of meetings, significant calls or discussions via electronic communications.
- Save documents to FileSite (unless otherwise specified by local business processes) in an appropriate Records Folder, with a fully and accurately completed document profile.
- When restricting access to documents in FileSite, where possible, grant access to groups rather than named individuals. This ensures continuous access to the right people as colleagues join, move and leave the Bank.
- Save email communications and other important electronic communications to FileSite – if they are a record or if they may be needed for more than six months. For further guidance, see >**details on 'My Service'**.
- Complete relevant training, when asked to do so (see >**e-learning site**).
- If you have line manager responsibility, ensure that those leaving your team save, as appropriate, their emails and documents beforehand.

Sharing information within the Bank

The information held by the Bank is one of its most important assets. Information needs to be shared actively within the Bank to allow it to be used effectively. In some cases, there may be contractual or other legal or policy reasons to restrict access to information internally (eg market sensitive information). We must understand when restricting access is necessary and how to achieve it. We trust our colleagues to be aware of these restrictions and to handle the information they receive properly (see also Being safe and secure).

Key considerations for sharing information internally are in the **>Internal information sharing policy.** In particular:

- Proactively share information with colleagues who have, or may have, a need to know it; do not just assume they will find it.
- Ensure you have stored your information promptly in an appropriate system and location where it is accessible to others, describing it appropriately and granting access to appropriate 'groups'.
- Understand the types of information or circumstances where restricting access to information is necessary.

External engagement

Engagement with external contacts is a core part of achieving the Bank's mission. As a result, many of us develop external business relationships and participate in external meetings and committees on behalf of the Bank. This helps us obtain information for policy making and supervision and allows us to impart information to further our mission in a wide variety of ways.

If you are attending external meetings on behalf of the Bank or speaking with external contacts, please ensure you are familiar with the **>external engagements guidance**. If you are dealing with a group of market participants, the related **>competition law guidance** will also be relevant.

Keeping accurate and complete records of business activities, as set out in the above requirement, is important when engaging externally. We are accountable for the information and advice we give, and for acting appropriately on the basis of what we learn.

The requirement for 'escalating external misconduct concerns' (see below) applies if we learn of relevant matters when engaging externally, and we need to remain alert to this possibility.

If discussions during a meeting begin to stray onto topics which you consider inappropriate and/or could give rise to some form of reputational harm to the Bank you should take action. Silence may erroneously be taken as consent or approval. You should request that your concerns are formally registered in the minutes or record, unless there is a 'tipping off' risk (see page 21). Feel empowered to leave the meeting, if you consider it appropriate. In such circumstances, inform your line management promptly, record the details in writing as soon as possible, and follow the escalation process (see below). Legal Directorate may also need to be informed.

Information held by the Bank is one of it's most important assets.

Disclosing information outside the Bank

While we have a duty to handle and protect information appropriately (see Being safe and secure), it is often appropriate to disclose information outside the Bank – to support our mission, policies and statutory functions. Before doing so, we must ensure that we comply with relevant controls, including legal, contractual and other obligations relating to the information. Particular requirements apply where the information was obtained from or relates to third-parties.

We protect the information we hold by classifying, storing and handling it correctly, and disclosing it only with the right authority – where there is an appropriate business need to do so – and making clear to recipients any restrictions that may apply.

Before disclosing information externally, you need to understand the nature of the information so that you handle it in accordance with the Bank's policies and obligations. This includes understanding:

- how the information was collected or produced;
- if received by the Bank, whether there is legislation or a contractual or other agreement that would limit onward disclosure;
- who you are intending to send the information to and for what purpose.

If you need further guidance, speak to your manager in the first instance. Other sources of help include: those in the Bank responsible for the particular information; subject matter experts; Security and Privacy Division ('SPD') and the Legal Directorate. Further advice on who to contact may be found >**on the intranet**.

Freedom of Information Act

Like other public bodies, the Bank is subject to the Freedom of Information Act 2000 (the FoI Act) and is accountable to the Information Commissioner for its compliance. We have a duty to respond to Freedom of Information (FoI) requests from the public where information is held and not subject to exclusions or exemptions set out in the FoI Act. This applies whether or not the request specifies the FoI Act.

If you receive a written request for information from someone outside the Bank, you will need to refer this to the Information Access Team promptly, in accordance with the >**Freedom of Information policy** (data protection requirements may also apply).

Anyone in the Bank could receive a written request for recorded information (for example, by letter or e-mail) so you need to:

- Ensure you are able to identify incoming written requests that meet the criteria of an information request under FoI.
- Understand the central referral procedures and send any information requests that meet the criteria to the Information Access team.
- Promptly complete relevant training, when asked to do (see >**details on the intranet**).

We protect information by classifying it correctly and disclosing it only with the right authority.

Public, press and media engagement

How we communicate is integral to our mission. We are open, honest and straightforward in our dealings with the public, Parliament and the press. Comments from any of us who work at the Bank can carry great weight.

The key requirements are:

- If you are contacted directly by someone from the media, including bloggers, please refer them to the Press Office in the first instance. Be wary of media 'cold calls'.
- The content of any planned interaction with media contacts, including bloggers, needs to be cleared by the Press Office each time it is used. Follow the policy on >**Dealing with the media**.
- Only interact with journalists or other media contacts on Bank matters, including via blogs or chat rooms, if you have the prior approval of the Bank's Press Office for the interaction. Please also exercise judgement in your social interactions with media contacts.
- If you are invited to speak at any external speaking engagement, you will need to consult the external >**Speaking engagements guidance**. You may need Press Office approval before accepting, for example if the media is likely to be present or interested.
- If you wish to publish a staff working paper or an article in an external academic journal or similar publication, you will need to follow the >**'Staff working papers and journals' process**.

Social media

When using social media in a personal capacity you must be mindful not to leave yourself and/or the Bank open to unwanted attention or reputational harm. Information given may be confidential and even when seemingly harmless could benefit cyber-attackers.

If you use social media, ensure that you are familiar with the requirements in the social media section of the >**SPD Conduct Policy**. If you are unable to satisfy a requirement detailed in this policy, you can apply in advance to SPD for a concession.

The key requirements are:

- Do not use a personal social media account to conduct Bank business.
- Do not comment on social media on matters directly within the Bank's mission (eg policy matters, interest rates, supervision of firms). For the foreseeable future, you should also be extremely cautious about comments relating to Brexit, so many aspects of which have an impact on the Bank's work and remit. Insofar as you comment about wider matters that are broadly within the interests of the Bank, please be clear you are giving your personal view.

  Regardless of whether you mention your Bank employment in such posts, readers may still be able to make the connection, and could perceive your comments as those of the Bank.
- Do not use your Bank email address to register for a social media account, unless for Bank business approved by your HoD in advance.
- Do not include excessive or sensitive information about your role at the Bank or your skills and experience in your social media profile.
- Do not post pictures or videos of the interior of any Bank premises without permission from Press Office, clearance from Security and a clear business justification. (Also, taking pictures or videos of the interior of Bank premises requires permission, see >**Being safe and secure**). Take care that confidential information is not in view while video-conferencing.

Public comments from any of us who work at the Bank can carry great weight.

Escalation of external misconduct concerns

We have contact with many parts of the financial sector and many people who work for financial sector firms. Through these contacts, we may occasionally pick up evidence or indications of misconduct (such as fraud, dishonesty, or market abuse). Equally, these contacts may allege misconduct by third parties. We should report such matters promptly. PRA colleagues also have particular responsibilities in relation to individuals who work in the financial services industry and who approach the PRA with concerns about their employer or other firms or individuals.

Local areas, such as Markets and Banking, also have an embedded escalation policy for external misconduct concerns, to be followed in addition to the general approach specified here.

Have you received evidence or indications of external misconduct in the financial sector? If so, follow these escalation procedures:

- Try to make sure that you clearly understand the nature of the allegations and the detail of the activity which gives rise to suspicion.
- Record it clearly and concisely in an email in line with the Standard for Creating Notes for Record.
- Send it to your HoD, Director or Executive Director, or your local compliance team who will liaise with the **>Intelligence and Whistleblowing (IAWB) Team** as appropriate.[2]
- Save the email appropriately.
- Do not tell the relevant person that you have raised a concern about them or their firm (in some circumstances this could be seen as 'tipping off').

Your HoD, Director or Executive Director will also advise you on how to manage the relationship with the relevant person or firm thereafter.

Have you been informed of an allegation of external misconduct by someone else eg outside the financial sector? If so, as well as the steps outlined above, you should also:

- Explain to them that, although the Bank may pass this information on, they should also approach any relevant regulator directly with their concerns and with any evidence they have.
- Record that you have done this.

We should all feel empowered without any fear of retaliation to escalate concerns about malpractice or misconduct.

2 The IAWB Team provides a service for those who wish to raise concerns about suspected wrongdoing, risk or malpractice in the financial services sector. Members of the public can contact them to disclose concerns about a firm or person employed in the sector. Bank employees and contractors and certain other people contacting the IAWB (such as an employee or ex-employee of a financial services firm regulated by the Bank) have protection under the Public Interest Disclosure Act 1998.

Being safe and secure

Safety and security are essential to our work. This includes how we handle information, use the Bank's IT, resources and systems and help ensure safety and security at the Bank's premises or when away from the Bank. We are responsible for the resources entrusted to us in the work we do.

Classifying, handling and protecting information

We take decisions for the public good based on a vast amount of information; much is confidential and/or sensitive and concerns or belongs to others.

We all sign a >**Declaration of Secrecy** when joining the Bank. This requires us to observe the strictest secrecy with respect to information of any kind acquired in the course of our duties relating to matters concerning the Bank and others with whom we have dealings (for example, the firms that we supervise).

Our systems and controls for safeguarding information depend upon us classifying and handling it appropriately in accordance with the >**Information Classification Scheme User Guide**. If you handle Bank Secret and Top Secret information, see the >**SPD Conduct Policy** for additional requirements.

The key requirements include:

- Label documents which are Bank Confidential, Bank Secret or Bank Top Secret with the appropriate classification on each page/sheet, and handle appropriately, reclassifying as necessary.
- When saving to FileSite, save with the appropriate classification and access controls.

The way we handle information, electronically or in paper form, must reflect its classification and our obligations with respect to different kinds of information (see also **Open and accountable** on record keeping, sharing information within the Bank and disclosing information outside the Bank).

One of the biggest risks around information is where we lose papers, or a laptop or other Bank electronic device, or make an e-mail error sending confidential information to the wrong recipient.

You must follow the Banks' policy restricting the taking of Bank Confidential paper out of the Bank (see page 25). If you lose Bank Confidential information or send it to the wrong recipient, you must immediately report the incident so that the Bank can take mitigating action.

Security, SPD, Bankwide Risk and Legal Directorate can all play a role in helping to recover information and mitigate such incidents. You should also consult guidance on what to do and who to contact if such a situation arises, including relevant legal and reputational issues see >**the data loss grabsheet**.

Privacy and data protection

We all have a responsibility to help ensure that the Bank complies with its legal requirements for handling personal data. These are set out in the General Data Protection Regulation (GDPR). In order to protect individuals when their personal data is handled, the Bank must adhere to the data protection principles set out in the legislation.

We all have a responsibility to protect the Bank's information.

Mishandling information can have far-reaching consequences.

Personal data means any information from which a living individual can be identified, whether directly from the information itself (eg a name, online identifier, location data) or when taken together with any other information. Mishandling personal data can have far-reaching consequences for the Bank, the person whose data it is and – in some circumstances – for us as individuals.

The Bank has data protection policies and awareness initiatives to ensure that we are mindful of our responsibilities and that the personal data the Bank holds is handled safely and securely. Further advice is available from the Bank's Privacy Team, in SPD. Please ensure you are familiar with the **>Privacy and Data Protection Conduct Policy**.

In our daily work at the Bank, we can protect personal data and the rights of individuals by following the data protection principles. Your responsibilities include:

- identifying and being aware of the personal data you handle in your role and keeping it appropriately secure;
- only accessing personal data if it is relevant to your role;
- referring information rights requests from individuals (even staff) about the data the Bank holds about them to data-protection@bankofengland.co.uk as soon as possible. Likewise related complaints;
- remembering that our own work or communications could be part of a subject access request (ie a request by an individual for a copy of the personal data held about them);
- reporting incidents, or suspected incidents, involving personal data immediately;
- consulting SPD Privacy if your role involves changing the way we collect or handle personal data;
- completing relevant training, promptly when asked to do so (see **>e-learning site**).

Using e-mail

When we use e-mail, we need to ensure we protect the Bank's information – particularly when e-mailing externally. We need to adhere to the restrictions on disclosing information outside the Bank (see above). Although there are technology safeguards, the only way to avoid mistakes – such as sending information to the wrong person – is to take extra care when sending e-mails externally; double-checking the recipient, attachments and classification.

When you are sending e-mail, remember:

- Do not send Bank Confidential information via e-mail unless the e-mail is classified as such, encrypted and sent to a trusted recipient.
- Do not send Bank information to a personal email address.
- Inform the recipient of restrictions about onward disclosure.
- Never send Bank Secret or higher classification information by e-mail.

When receiving e-mail, remember it is your responsibility to ensure that you only open e-mail attachments, click links or respond when you are expecting them or when they are from a known and trusted source. If you are not sure, report it using the 'Suspicious Email' button in Outlook.

You can find out more about **>classifying** and **>encrypting** e-mails.

Using Bank IT and other resources

As a public sector institution funded by the industry we regulate and the people we serve, we are all accountable for using the Bank's resources securely, efficiently and effectively.

As we work with IT on a daily basis, we need to follow these key requirements:

- Only use Bank IT equipment, not our personal equipment, for Bank work.
- Use Bank IT lawfully.
- Do not share, display or reuse passwords.
- Complete 'Cyber-7' and other relevant training, when asked to do so (see >**e-learning site**).
- Do not alter configurations or security settings on Bank IT equipment, or install unauthorised applications or software.

To find out more on how to use IT safely and securely, please see the >**SPD Conduct Policy** made under the >**SPD Charter**, particularly on 'IT use' and personally enabled devices. This includes a Monitoring Notice, which sets out the extent to which the Bank may monitor use of its equipment, explaining that you should have a limited expectation of privacy when using it.

We are permitted in certain circumstances to make limited, reasonable personal use of Bank IT resources, but not in a way that would conflict with our work or with the security and integrity of the Bank. If you have a Bank device enabled also for your personal use, please ensure you are familiar with the additional requirements in the 'Working with personally enabled devices' section of the >**SPD Conduct Policy**.

Safety and security at the Bank's premises

The Bank's premises are a safe and secure environment. SPD is responsible for maintaining physical security and the Property Division for maintaining health and safety. This also depends on all of us taking responsibility to remain alert to matters that look out of place or may indicate a security risk, informing the SPD of any concerns.

You support their work by following these requirements:

- You are encouraged to wear your security pass while on site at Bank premises.
- Remove your pass as you leave the premises – including when walking between the Bank premises at Threadneedle Street and Moorgate.
- If you invite visitors to the Bank – follow the >**requirements for visitors**. In particular, ensure your visitors know they must bring acceptable ID with them to be allowed access. Also, ensure they are escorted at all times when on Bank premises. You should feel empowered to challenge any unescorted visitor, and politely escort them to where they should be.
- Maintain a clear desk overnight, locking papers and laptops away. During the day when leaving your desk for a length of time, lock your computer screen and secure confidential information. Always store your token separately.
- You must comply with the restrictions on photography within any Bank premises as set out in the >**SPD Conduct Policy** (See also use of social media on posting photos on line).
- Ensure you understand >**the Bank's safety arrangements manual**, and complete the Emergency Procedures awareness training when asked to do so.

We help protect ourselves, colleagues and visitors by reporting promptly any issues or concerns about safety or security (see page 28).

We must ensure we use IT safely and securely.

Safety and security outside the Bank's premises

Safety and security is also a priority whenever we are working away from the Bank's premises.

If you are 'working away from the Bank', eg at home, in transit or abroad, the >**SPD Conduct Policy** sets out the steps you must take in order to help maintain information security.

Key requirements include:

- Be careful in the conversations you have outside the Bank – particularly in public spaces.
- Protect your laptop or mobile device with a privacy screen if using in public spaces, such as on trains. If you work as you travel, information must remain secure.
- Protect our sensitive information by printing the minimum pages necessary and only taking Bank Confidential documents off-site, in accordance with document-handling requirements, if you have appropriate permission, a business need to do so and subject to any additional local area policies or restrictions.
- In particular, only take Bank Confidential papers off-site overnight if you have recorded details in advance on the appropriate >**form** and you are permitted by bankwide and local >**policies**. Additional restriction will apply in areas of heightened sensitivity (eg Committees, EU withdrawal, Resolution, Stress-testing).

If you travel for work (business travel), or take Bank information or IT with you in personal travel, the 'Travelling' section of the >**SPD Conduct Policy** sets out what you must do to maintain information security when you travel.

Are you travelling to a 'high cyber-threat environment'? The current list of high cyber-threat environments appears >**on the intranet**. If travelling to such an environment, you will need to read the additional requirements in the 'Travelling' section, for example that you must not take your usual Bank IT equipment there.

Safeguarding against money laundering, terrorist financing and financial sanctions

As a financial institution, the Bank is committed to high standards of financial crime prevention and must comply with financial sanctions legislation. Under the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, Proceeds of Crime Act 2002 and the Terrorism Act 2000, we each have a statutory duty to disclose, as soon as reasonably possible, information that indicates money laundering or terrorist financing is occurring or has occurred. This could include suspicions about attempts to abuse the Bank's own processes in order to launder money or finance terrorists. This could also include indications that external institutions may be involved in, or instrumental to, money laundering or terrorist financing activity.

Within the Bank, the person responsible for investigating and reporting such suspicions is the Bank's >**Money Laundering Reporting Officer (MLRO)**.

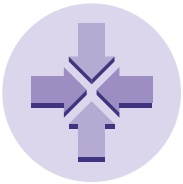
Whatever your role in the Bank, you are required to:

- Report to the MLRO or a Deputy MLRO, either directly or through your line manager, as soon as reasonably possible, any information that indicates money laundering, terrorist financing or financial sanction breaches may occur or have occurred.
- Complete relevant training, when asked to do so (see >**e-learning site**).

If your work involves speaking with third parties about financial institutions or markets and if you are part of the Bank's financial operations, you must also adhere to controls applicable to your role as set out in the Anti-money Laundering and Terrorist Financing Risk Standard and Financial Sanctions Risk Standard. See >**the Banks Anti-Money Laundering & Financial Sanctions Policy**.

Remain alert to matters that look out of place or may indicate a security risk.

Creating an inclusive and empowering culture



To support the Bank's mission we recognise the need to continue to build an inclusive culture where we can all contribute our best work. We want all colleagues to feel comfortable being themselves. We treat each other with respect.

We support each other in managing our time between work and personal life, and we embrace diversity and the benefits it brings.

Each of us should feel encouraged to raise issues or concerns.

Inclusion strategy

The Inclusion Strategy is an important part of delivering this culture and in supporting the Vision 2020 priorities within the Bank. The strategy creates a framework to bring together three strands of work:

- **Diversity** – to reflect the society we serve, make better decisions, avoid unconscious bias and ensure diversity of thought;
- **Community** – to maximise the Bank's positive impact and influence in our community;
- **Wellbeing** – to support colleagues' mental and physical health, to enable them to bring their whole selves to work.

There are Directorate, Deputy Governorship and Bank-wide inclusion initiatives and you can learn more about the Bank's >**Inclusion strategy**.

Discrimination, bullying and harassment

Our workplace should be free from all forms of discrimination, bullying and harassment. We recruit, hire, develop, promote, manage and provide conditions of employment without regard to age; disability; gender reassignment; marriage and civil partnership; pregnancy and maternity; race; religion or belief; sex; sexual orientation. We are all personally responsible for the avoidance of discrimination under the Equality Act 2010.

If you feel you have been discriminated against, harassed or bullied, or have seen anyone else treated in such a way, raise the matter with your manager if appropriate or the HR Employee Relations Team under the Diversity policy or the Anti-harassment/bullying policy. See also the Speak up policy. See >**the policies and guidance on the intranet**.

Speaking up

We are all encouraged and empowered, without any fear of retaliation, to speak up about malpractice or misconduct or to raise serious concerns if we feel the Bank or anyone in it is contravening the policies in Our Code. We can raise these concerns through line management or through the >**Speak up policy**.

We are committed to supporting those who speak up. It doesn't matter if they are mistaken. We do not tolerate any victimisation or harassment of those who speak up. They will not lose their job for speaking up. If you speak up and ask us to protect your identity we will do so unless otherwise required by law. If it becomes impossible to investigate without disclosing your identity, we will discuss this with you before taking the issue further.

What do I need to disclose or seek approval/permission for?

Conflicts of interest checklist

Disclose and keep up to date in HR Connect

Disclose to the Secretary or HR

Seek approval before:

If offered entertainment and gifts:

Other disclosures/permissions

If your personal circumstance change materially:

If you want to take part in a media discussion or speak at an event where the media is present:

If you want to take a photograph within the Bank:

If you want to take Bank Confidential papers off-site overnight:

How can I raise or report matters of concern?

If there is something of concern that you may need to report, typically the first thing to do is to discuss the matter with your line manager, if available.

Breaches of Our Code or related staff conduct policies	Report via the incident management system or direct to the Compliance Division via **ourcode@bankofengland.co.uk**
General security matters	Report to the Security Desk **020 760 13332** (24 hour) **SecurityMatters@bankofengland.co.uk**
Bullying, discrimination or harassment	Discuss with HR Employee Relations Team **ASKHR@bankofengland.co.uk**
Data protection breach or any loss of Bank Confidential information	Report by e-mailing **Dataloss@bankofengland.co.uk** Outside working hours telephone the Security Desk **020 760 13332** (24 hour)
Freedom of Information request	Forward to the Information Access Team **Communications-Information-Access@bankofengland.co.uk**
Money Laundering concerns, or financial sanctions issue	Report to Money Laundering Reporting Officer or deputy Money Laundering Reporting Officer **MLRO@bankofengland.co.uk**
Grievances (*dissatisfaction with your treatment in the Bank, or problems or concerns about your work, working conditions or relationships with colleagues*)	Discuss with HR Employee Relations Team **ASKHR@bankofengland.co.uk** (NB Grievances are governed by the Staff Handbook, not Our Code)
Speaking up (internal whistleblowing: serious concerns about disregard of Bank policies, a risk to the Bank, a possible fraud, misconduct or malpractice)	Discuss with line manager, nominated representatives listed in the policy or Deputy Secretaries **Deputy.secretaries@bankofengland.co.uk**
Escalation of external misconduct concerns	Your HoD, Director or **IAWB@bankofengland.co.uk**

Who do I speak to for further information about the policies?

If you have a question about a policy under Our Code, you could:
Speak to your line manager or HoD

Email **ourcode@bankofengland.co.uk**

Contact the relevant policy owner/expert, as follows:

Policy	Policy owner/expert
– Conflicts of interest policies (Personal relationships, financial relationships, personal financial transactions, directorships, community and charity roles, political activities) – Entertainment and gifts policy – Secrecy declaration – Speak up policy	The Secretary's Department Deputy Secretaries **Deputy.secretaries@bankofengland.co.uk**
Other employment policy Bullying discrimination and harassment Diversity Wellbeing and inclusion	HR Employee Relations Team **ASKHR@bankofengland.co.uk**
Record keeping policy	The Secretary's Department – Records Management Team **BankRecordsManagementTeam@bankofengland.co.uk**
SPD Conduct Policy Privacy/data protection Security Vetting Policy	Security and Privacy Directorate (SPD) **SPD.Policy@bankofengland.co.uk**
Social media	Jointly with Communications Directorate for social media
Freedom of Information	Information Access Team **Communications-Information-Access@bankofengland.co.uk**
Public, press and media engagement	Press office **Press OfficePress@bankofengland.co.uk**
Money laundering, terrorist financing or financial sanctions	Money laundering, Operational Risk & Compliance, Markets & Banking COOD **MLRO@bankofengland.co.uk**

How we use your information

Information we collect

As part of the policies under Our Code, you may be required to provide personal data to the Bank.

From time to time, the Compliance Division may request further information from you about the matters you have disclosed or where you have sought prior approval, for example relevant bank statements or appropriate tax returns. You are expected to retain or have access to supporting information on financial relationships and personal financial transactions for at least five years.

Why we need your personal data

We collect your personal data for the purposes of ensuring compliance with Our Code. This is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Bank. In particular, we use your data in order to:

- understand whether there are any actual or potential conflicts of interest between your work and your personal life, or any risk of perception of undue influence; and
- ensure appropriate mitigation where such matters arise.

In the case of special category personal data such as political opinions, it is in the substantial public interest to process this personal data.

What we do with your personal data

Information you provide will be treated as strictly confidential, and will be stored securely.

Information you provide in relation to an approval request or disclosure may be reviewed by the Secretary's Department, Local Reporting Officers (for personal financial transactions), the Compliance Division and Internal Audit. It may also be necessary for Our Code related information to be made available to HR, the Security Vetting team, the Legal Directorate, local management and relevant senior management, on a 'need to know' basis. Information relating to Policy Committee members may also be made available to the relevant Committee and its secretariat.

We will retain your personal data for the periods specified in the Bank Records Classification Scheme.

For more information, see the Bank's >**How we use staff data notice**.

Your rights

You have a number of rights under data protection laws. For example, you have the right to ask for a copy of the personal data the Bank holds about you. This is known as a 'Subject Access Request'. You can ask about how the Bank processes or deals with your personal data, and you may also have the right in some circumstances to have your data amended or deleted.

To find out more about those rights, to make a complaint, or to contact our Data Protection Officer, please see >**www.bankofengland.co.uk/legal/privacy**.

BANK OF ENGLAND

Our Code
Version 1.0, June 2015
Version 1.1, September 2016
Version 2.0, September 2017
Version 2.1, September 2018