Bank of England

Our Code

January 2024

I've long felt that working at the Bank provides a unique opportunity to 'promote the good of the people of the UK'. Our ability to achieve that mission depends on public trust, and a belief that we will demonstrate the highest standards of public service.

In that respect, Our Code is in many ways, the most important document we have. It tells us how we put standards of public service into practice by: acting with integrity and impartiality; being open and accountable; being safe and secure; and promoting a diverse, inclusive and empowering workplace. It also outlines the policies and requirements that support those standards and shows where we can go for further guidance and advice.

All of us who work here at the Bank have to adhere to Our Code, and we attest to it on joining the Bank and annually. This is how we confirm we have read and understood the Code, and we are up-to-date with the relevant disclosures and approvals.

Our Code also describes how we treat others and how we expect to be treated in line with **Our Bank Behaviours**: acting inclusively by earning trust; driving growth by overcoming the fear to speak out; and delivering outcomes by holding ourselves and others to account.

In that regard, I want to underline how important it is that you raise any concerns you have, or report any breaches of policy you think might have occurred. Our Code explains how to do this, including through **Speaking up**. You need only tell us that something needs to be looked into. We will do the rest, and I can assure you that anything you say will be treated with the strictest confidence.

Thank you for taking the time to read Our Code, and for your continued commitment to uphold the highest standards of public service.

Our reputation, and the trust of the public we serve, depends on it.

Andrew Bailey

January 2024

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, key policies and their underlying 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 and approvals. This enables others within the Bank to decide whether these disclosures could represent a perceived or actual conflict of interest, and how any such conflicts should be handled.

Being open and accountable…

focuses on policies about how we communicate and keep appropriate records. It includes policies on record keeping, internal and external information sharing, escalating external misconduct concerns and audio or audio-visual recording of meetings.

Being safe and secure…

covers some of the fundamentals of how we work, in relation to operational, conduct and security risks, including the risk of financial crime. If we fail to work in a safe and secure way, we could cause operational, reputational and legal harm to the Bank and undermine our mission. Mishandling firm sensitive or personal data could also have negative consequences for individuals.

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 our policies.

Attestation

You must attest to Our Code annually, confirming that you have read, understood and complied (as appropriate) with the requirements in all Bank-wide policies and summarised 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. Attestation is completed using the Our Code Compliance system.

Compliance and breaches

You are expected to protect yourself, colleagues and the Bank by identifying and reporting breaches[1] of Our Code and other Bank policies promptly. If you realise you have breached – or suspect that you might have breached – a requirement in a policy please report it to **AskCompliance** as quickly as possible, so that the issue can be redressed under the Bank's **>Breach management policy**.

You should be aware that failing to discharge your responsibilities could lead to disciplinary or other action; although the Bank gives credit for you taking prompt responsibility for your mistakes.

Managers should encourage a culture of openness and integrity around reporting breaches, ensuring their staff understand that prompt and full reporting is an integral part of managing breaches. Guidance for this can be found in the **>Our Code and compliance guidance for managers**.

There is useful information in the sections: 'Mandatory courses we need to complete', '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?'.

As well as Our Code, we must also comply with the Staff Handbook and other Bank policies in the **>Policy bank**.

You are required to:

- Know, understand, and comply with the requirements in our Bank policies, of which the key ones are summarised in Our Code and ask questions if you need clarification or advice.
- Gain permissions for any exceptions or make any disclosures that may be required.
- Confirm annually that you have read, understood and complied (as appropriate) with the requirements in internal Bank policies.
- 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 (internal whistleblowing) **>Speaking up policy**.

Acting with integrity, demonstrating impartiality

Integrity is one of the Seven Principles of Public Life.[2] 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 'Classifying, handling and protecting information').
- 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 independently 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 any actual or perceived conflicts when you change roles or teams within the Bank.

You must use the Bank's resources responsibly, ensuring value for money. When incurring travel and expenses costs on behalf of the Bank, you must ensure that these are reasonable and in accordance with the Bank's **>Travel and expenses policy**. For other expenditure, if you purchase or authorise the purchase of goods or services on behalf of the Bank, you must follow the requirements of the Bank's **>Procurement policy**. Failing to do so exposes the Bank to financial, legal and reputational risk. Where contractual arrangements are below £500 the **>Non-travel expenses policy** applies. This policy requires you to raise a purchase order, unless there is business justification for incurring the expenditure by another route. You must also adhere to the limits and conditions that apply to certain types of non-travel related expenditure.

The **>Working from abroad policy** outlines the requirements to follow when planning to work from abroad, as a result of an employee-instigated trip. We can work from abroad for a total of 40 working days in any rolling 12-month period (pro-rated for part-time working patterns). Executive Directors are required to attest annually that staff and managers in their areas are adhering to this policy.

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 or disclose immediately in the Our Code Compliance system 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.

On appointment and annually as part of attestation, Court members and members of the statutory policy committees (including Executive Directors who are members of a statutory policy committee) 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.

Personal relationships

We are required to disclose certain close personal relationships within the Bank or in specific roles externally, including having active discussions about prospective employment with certain types of firms. This is to ensure that the risk of an actual or perceived conflict of interest can be managed.

Where a close personal relationship with someone working in the Bank exists, adjustments may be needed. This is particularly relevant for example in areas of the Bank's operations where there is dual control of assets or signature panels for release of payments. You must not participate in a decision to hire, directly or indirectly manage, or contribute to appraisals, pay and promotion decisions of someone with whom you have a close personal relationship (as defined below).

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.

You must disclose in the Our Code Compliance system and **notify** your line manager of each of the following **>Close personal relationships**. New or updated declarations may be required, for instance, because your living arrangements have changed, and this makes the potential for actual or perceived conflicts to arise more acute. For all personal relationships that are disclosed, your line manager will consider whether a risk arises, and if so, what mitigants may need to be put in place. **You must disclose the following:**

- 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; and
  - holding a national elected public office (MPs, the Scottish Parliament, the Welsh Parliament, the London or Northern Ireland 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.
- This could be with individuals working in or outside the Bank. Such conflicts relating to a particular situation are likely to arise only occasionally.

Disclosure protects staff in exactly the same way as personal financial transactions and entertainment and gifts reporting. Where you have a close personal relationship with someone working for an organisation with a financial interest in the activities and/or decisions of the Bank, this may mean that you cannot take on or continue in some roles. It may be necessary to discuss with you a transfer to another area or to other work, or avoidance of particular work, in order to protect you, the person with whom you have declared the relationship, and/or the Bank. This would be in full consultation with the parties involved. It could mean for example; you are not directly supervising a Bank-regulated firm; not being involved in contingency planning for a Bank-regulated firm; or not having a role that requires being part of the Monetary Policy Committee (MPC) or Financial Policy Committee (FPC) insider lists.

If you are unsure about whether to disclose such a relationship, please seek guidance from the **Conflicts Team** 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, Deputy Secretary or Conflicts Team in the Secretary's Department may allow an exception to the disclosure requirement.

Discussions on prospective employment and restricted duties

Actual or potential conflicts of interest may arise where we are seeking a role with a prospective new employer and may also need to be disclosed.

It is **mandatory for all of us** to disclose with reasonable advance notice, when having **active two-way discussions about prospective employment** (ie interviewing) with:

- a Bank-regulated firm;
- a significant dealing counterparty of the Bank;
- a firm that you have contact with as a Bank supplier; or
- any other organisation that might create a conflict of interest, such as consultancy and legal firms providing advice or services to Bank-regulated firms.

You must disclose this as a personal relationship in the Our Code Compliance system so that your manager is aware, and any potential conflict of interest can be managed appropriately. If you do not wish to notify your line manager of your active discussions with one of these types of firms, you must make the Conflicts Team aware promptly, and take advice on the management of any conflicts that may arise.

The Conflicts Team will maintain your confidentiality 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. The Conflicts Team can help determine whether you need to alert your line manager in order to mitigate any such risks. They may also provide advice on the management of any conflicts that may arise.

In order to manage perceived or actual conflicts of interest which may arise when a member of staff is leaving the Bank, the **>Restricted duties policy** sets out restrictions which may be applied to all staff upon resignation.

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.

We must not under any circumstances seek to make a profit or avoid a loss by making use of information acquired in the course of our duties at the Bank. We should exercise caution in the management of our finances.

Dealing in securities on the basis of inside – ie unpublished, price sensitive – information is a criminal offence.

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 (eg a spouse, partner or child) 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 the Our Code Compliance system 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.
- Direct holdings of individual gilts.
- 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 (FSCS) – currently £85,000 per person per firm. (If you have accounts that are covered by temporary high balances protection under the FSCS scheme – up to £1 million for six months for certain life events – you are not required to disclose this).
- 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 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 advice from the Conflicts Team in the Secretary’s Department before making a declaration.

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 a transaction before approval is granted or if approval has been refused.

You must obtain advance approval via the Our Code Compliance system giving at least five working days' 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. Approval must be sought once a mortgage offer is received and before it is accepted.
- **Dealings in exchange-listed securities and related investments (including gilts), 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.
- **Setting up or transferring a personal pension plan** and taking or approving decisions relating to the investments within such a plan. Switching between funds within the Bank's Supplementary Pension Plan does not require approval.
- **Transferring more than £5,000 from a bank or building society where you hold a balance greater than the FSCS limit** (currently £85,000 per person per firm) to an account at another institution (including National Savings and Investments). You should not split up financial transactions in order to circumvent this requirement. You do not need to seek approval for transfers made within the same institution, or for payments made to others for goods and services.
- **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. Where you have not previously sought approval, but you wish to reverse a transaction in foreign exchange made within six months because of market movements, you do need to seek approval.
- **Carrying out any other financial transaction that could reasonably be seen as 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. During 'quiet periods'[3] certain transactions by those on the insider lists for MPC and FPC meetings will not ordinarily be permitted.

If you are unsure about whether to seek approval for a personal financial transaction, please seek advice from the Conflicts Team.

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

Exemptions where investments are under full discretionary management

Exemptions from the full requirements of the Policy are available where your investment assets are managed by a personal portfolio manager who has full discretion over investment decisions on terms that have been specifically approved in advance by the Secretary or Conflicts Team.

We require you to sign up to a set of undertakings to provide assurance that day-to-day control over all investment decisions – which include security selection and asset allocation – would rest solely with the portfolio manager once the mandate has been agreed, and that you will not provide any instruction relating to, or otherwise directly or indirectly influence, such decisions.

Where you are selecting specific investments or collective investment funds yourself, even where these are index-tracking funds, this would not be considered full discretionary management.

Where a discretionary management arrangement has been approved by the Secretary, the restrictions and requirement for pre-approvals in the Policy no longer apply.

Additional requirements and guidance for members of Court and the statutory policy committees

In addition to the requirements set out above, Court members and members of the statutory policy committees, (including Executive Directors who are members of a statutory policy committee) must report their stock of financial assets and liabilities annually to the Secretary.

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 material investment portfolio, you are strongly advised to place it under full discretionary management on terms approved in advance by the Secretary.

Members of this group are expected to make themselves aware of any transaction of the nature covered by these rules by close family members (ie spouse, partner, minor children or other close family who live within the same household) that could embarrass the Bank or harm its reputation.

Members of this group are expected to keep records of their personal financial transactions and of the aforementioned close family members, for at least five years, and on request make them available to the Bank.

Prohibited transactions

You must not carry out transactions that might embarrass the Bank or harm its reputation. Certain kinds of transaction are never allowed:

Do not acquire financial instruments (such as debt, equity, or derivatives) in any entity regulated by the Bank, including PRA-regulated firms, or their financial holding companies.

If you joined the Bank with holdings in an entity regulated by the Bank you may retain them, but you must declare your holdings under the financial relationships section of the Our Code Compliance system. You must not acquire more or actively manage them. 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 to make a profit or avoid a loss in the short term) including transactions 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, UK indices/sectors or economic variables of direct interest to the Bank and its forecasting processes (eg commodity or currency markets) or the UK equity market as a whole.

Do not invest in collective investment schemes that are unduly weighted towards investments in the financial services industry. Ordinarily this means portfolios should not be more than 35% invested in financial services securities.

In exceptional circumstances, additional restrictions on transactions may be imposed on relevant staff during periods of significant stress in financial markets. This would be agreed by the Governor and the Secretary and communicated to the individuals concerned.

Roles and activities outside the Bank

Directorships

We are not allowed to become directors of companies without the Bank's advance consent.

Permission will not normally be granted for you to become a director (whether executive or non-executive or otherwise) of a company engaged in business, as this can give rise to a range of financial, legal and reputational risks. Permission **will not be** granted in the case of organisations engaged in financial markets or Bank-regulated firms and their holding companies. You may be permitted to take on the directorship of a non-trading company – for example, one set up by leaseholders in a block of flats to acquire or manage the freehold. Directorships of social enterprises or charities may also be permitted as these raise fewer concerns, but advance approval is still required. If you wish to become a director of a company (whether non-executive or otherwise), approval is required in advance. Any actual or perceived conflicts of interest will need to be discussed and resolved.

You must seek approval via the Our Code Compliance system before becoming a **>Director**.

Your request will be considered by the Conflicts Team in 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 the Our Code Compliance system. Examples include director trustees of BE Pension Fund Trustees Limited.

Community and charity roles

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

You must disclose via the Our Code Compliance system before taking on a **>Charity or community role** with legal duties or formal responsibilities such as:

- a charity trustee or member of a charity's investment committee; and
- a school governor.

Your disclosure will be reviewed by the Conflicts Team in the Secretary's Department and your line manager.

If the nature of the charity/organisation and its activities changes, or if your role changes, you should notify the Conflicts Team and your line manager.

Please note that if you make or advise on financial decisions as part of such a role then the Personal Financial Transactions policy 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, leading a Bank club or society, 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 your wellbeing and your ability to deliver your work at the Bank to the necessary standard due to time commitments.

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

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

Other employment

Most people at the Bank do not have additional employment. You must seek the approval of your HoD before you take up any other employment while you are working at the Bank. This is in case it may give rise to a conflict of interest, a perception of advantage, a reputational risk to the Bank, or otherwise be considered detrimental to the Bank's interests.

For the purposes of this policy, 'any other employment' covers any paid or unpaid work undertaken for another employer under contractual obligation (other than where you are volunteering for a charity or community role), for example, working as a professor or lecturer in academia, or as an adviser to research groups (where unrelated to your Bank role). It also covers self-employment as a sole trader, within a partnership or via a limited company in which you are a shareholder.

Your HoD will also need to consider whether this might adversely impact your wellbeing and 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 have appropriate authorisation to undertake any other employment while you are working at the Bank. You must discuss any other employment with your line manager and seek approval from your HoD via the Our Code Compliance system from your HoD before taking on **>Other employment**.

If approved, you must ensure that your other employment is not undertaken in Bank time, when you are expected to be working, or using Bank resources (including your Bank email address).

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:

- take up employment with a Bank-regulated firm;
- 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; or
- receive any commission or gratuity from such a broker or dealer for recommending business to them.

Political activities

We recognise that, in engaging with your community, you may want to engage in political activities. Political activity here refers to active engagement in:

- **Party political matters** such as standing in local or national elections, being involved in campaigning (on-line and in person), raising money for a political party, or being on a local party management committee. It does not cover simply being a member of a political party, or providing administrative support to it, such as delivering leaflets.

- **Matters of national political controversy relating to your work at the Bank and the role of the Bank**, where this could call into question your own political impartiality in the way in which you carry out work for the Bank, or the apolitical status of the Bank itself. This covers speaking publicly or publicly expressing views on such matters on any public platform (including to the media, on the internet, via books, articles or other medium).

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 **>Political activity**:

- **You must notify** the Conflicts Team and your HoD via the Our Code Compliance system in advance if your political activity is likely to include involvement in party organisation, fundraising or campaigning (eg door-to-door canvassing).
- You must avoid any suggestion that the Bank supports or endorses your political activity. This means:
- you must not engage in political activity while on duty, or using Bank premises, systems or resources; and
- you must make clear that your involvement is solely in a personal capacity.
- You must not publicise that you work for the Bank in connection with it.
- You must avoid speaking publicly or publicly expressing views on matters of national political controversy relating to your work and the role of the Bank where this could call into question your own political impartiality or the apolitical status of the Bank itself; and
- you must comply with the Bank's **>External communications and engagement policy** when engaging in political activities, particularly where there is a risk of the Bank being drawn into a matter of political or public controversy) and raise any questions about media contact or public debate with the Executive Director, Communications or the Chief Press Officer.

You must seek consent in advance from the Secretary via the Our Code Compliance system, giving at least three months' notice, if you wish to stand for local or national elected office. In exceptional circumstances, the Secretary may allow for a shorter notice period. You should also make your HoD aware of your request.

The Secretary may consult local management and Governors as necessary to consider any sensitivities arising from your work and any risk to the Bank's reputation for impartiality.

If you are selected as a party candidate for membership of the House of Commons, the Scottish Parliament, or the Welsh, Northern Irish or London Assemblies or for any other remunerated 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 from the Bank with immediate effect.

If you are elected as a member of a local authority or similar body, you may be allowed to remain employed by the Bank.

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 giving and receiving 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 impartiality and to protect against any suggestion of impropriety.

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.

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.

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.

Entertainment and gifts must be fully and accurately recorded for reporting in accordance with arrangements approved by the Secretary's Department. In general, this means using the Our Code Compliance system for entertainment and gift reporting. This includes recording gifts you have accepted, that you are subsequently not given permission to keep. This process is subject to audit.

Where necessary, business areas may, with the prior approval of the Secretary, adopt **additional** local business area rules for gifts and entertainment to suit the particular circumstances of their work. The rules contained in the **>Bank-wide entertainment and gift policy** are the minimum and apply where no local variations are in place. 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 offered at a meeting, such as tea, coffee and biscuits do not fall under these rules.

You should 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 (eg a procurement decision); or
- liable to bring you or the Bank into disrepute.

'Excessive' includes offers of entertainment that are disproportionately lavish (such as invitations to expensive events), over-frequent (pattern of invitations to one area from a particular organisation that, taken together, appears inappropriate), or too time-consuming.

Please decline any invitations from firms regulated by the Bank or the Financial Conduct Authority (FCA), or from professional advisers 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 accepted in an official Bank capacity (eg whether through your day to day Bank role or your role on a Bank employee network) and not a personal capacity should be seen as institutional and reported accordingly (eg where a firm is paying for the hospitality). **Invitations from personal friends that are not offered in an official capacity and do not involve corporate hospitality (ie not paid for by a firm) do not need to be reported.**

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. For example, you should consider if the invitation is from a Bank or FCA regulated firm; from professional advisers; or from an organisation that you have contact with as part of your role.

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

Gift rules

You should 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 solicit gifts from a Bank supplier for yourself or for any other purpose.

You must not accept:

- cash or retail vouchers (except for commemorative coins/specimen notes); and
- electronic devices (for security reasons).

You may keep a gift up to the value of:

- £30, if your HoD gives permission; and
- £100, if the Secretary (or the Conflicts Team) gives permission.

No gifts worth more than £30 (such as hampers or ‘goodie’ bags) should be broken up into smaller portions to comply with the £30 rule.

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, then you must;

- give it to charity directly if the value is under £30;
- pass it to **Community** for disposal for charity if the value is over £30;
- alternatively, if it has a value less than £100 it may be disposed of for charity under local arrangements (eg raffle) approved by your HoD; and
- gifts whose value is likely to be in excess of £100 should be passed to the Community team for the benefit of charitable organisations.

Personal data and changes of personal circumstances

Everyone who works at any of the Bank’s sites is required to have an appropriate level of security clearance for their role. This includes all employees, temporary staff, and contractors. In order to ensure your security clearance remains valid it is important to ensure the information it is based on is kept up-to-date. This means that you must make the Security Vetting Team aware of any changes in your personal circumstances. This includes reporting mental health conditions and abuse, misuse or addiction issues.

It is very unlikely that disclosing mental health conditions will affect your security clearance. Each case is dealt with on a case-by-case basis in consultation with the individual concerned. The Security Vetting Team are trained to deal sensitively and confidentially with any disclosures of mental health conditions. They understand that disclosure can be difficult, and they will work with the affected colleague to support them through the process. Further information on this, including a list of the mental health conditions to be reported, can be found in the **>Security vetting standard** and **>Vetting and mental health** FAQs.

You must complete personal data reviews when prompted and keep your personal data in the One Bank Service and Our Code Compliance system up-to-date.

You must complete actions directed by the Security Vetting Team, when requested.

You must disclose to the Security Vetting Team promptly details of **>Changes in personal circumstances** that may affect security clearance. The list of relevant changes in personal circumstances now includes:

- a change in partner, getting married or entering a civil partnership or co-habiting;
- a change in nationality (this could be newly acquired or renouncing a previously held nationality);
- receiving a court judgement;
- being arrested, bailed, summonsed, receiving a police caution, being charged with a criminal offence or being convicted (other than minor road traffic offences);
- a material change in personal or financial circumstances;[4]
- severe medical or psychological illness (specifically where it or its treatment may cause blackouts, issues regarding perception of reality, judgements or paranoia); and
- abuse, misuse or addiction issues for prescription or illegal drugs, or alcohol.

If you hold a Developed Vetting level clearance you need to declare all the above changes in circumstances, plus the following:

- changes in adult co-residents at your address. This includes any house sharers/flatmates over 18 who are in addition to your declared partner; or
- your personal travel to high cyber threat countries.

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.

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:

- 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.

- Complete relevant training, when asked to do so (within One Bank Service, navigate to Me **>Learning**).

Line manager responsibilities include ensuring all members of your team are meeting their record keeping obligations. This is particularly important when colleagues join and leave your team.

In addition, the **>Creating records of meetings, committees and calls policy** sets out requirements for the prompt creation of notes for record and/or minutes of discussions. It also specifies record keeping requirements for committees that the Bank sponsors or attends which include external participants.

Key requirements are:

- Create accurate and complete records of substantive discussions with internal colleagues and external parties.
- Create records promptly, no more than 10 working days after the discussion.
- Ensure the records are saved to an appropriate FileSite Records Folder.
- Contemporaneous notes (eg created in OneNote or handwritten) must be transferred to a Note for Record/Minute and stored in FileSite and should then be deleted/destroyed.
- For committees, Terms of Reference should be documented in FileSite.

As we continue to conduct many of our meetings online or as hybrid meetings using services, such as MS Teams, it is important to ensure you are familiar with the requirements of the **>Audio and audio-visual recording of meetings policy**. This policy sets out that meetings should only be recorded on an exceptional basis, with the prior approval of the meeting chair, the consent of others present and your line manager/HoD. The policy outlines when it is appropriate to make an audio or audio-visual recording of a meeting and specifies the technology which must be used and how recordings should be saved, protected and shared.

Data management and analytical processes

Most things we do in the Bank depend on data. Our data analytics outputs are used in decision-making and publications. Examples include tables, charts, dashboards, results embedded in committee papers and derived data sets.

It is important that we can:

- find our data sets and data analytics outputs;
- interpret them correctly;
- trust them enough to use them; and
- manage the risks arising from producing and using them.

The **Data management policy** explains your responsibilities for managing our data sets.

The **Analytical process policy** explains your responsibilities for managing the analytical processes that produce our data analytics outputs.

Remember: when you create a data set or analytical process, please register it following our registration process as set out on **Data and process registration** intranet page.

Internal and external information sharing

The information held by the Bank is one of its most important assets. Information often needs to be shared actively and widely within the Bank to allow it to be used effectively. But 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 and external information sharing policy**. In particular:

When sharing internally:

- Information should flow freely within the Bank to enable effective decision-making and to ensure the delivery of the Bank's mission.
- Access to sensitive information must be restricted to minimise risks of inadvertent or deliberate disclosure to unauthorised Bank staff or external contacts.
- Take action to proactively share information; do not just assume colleagues will find it.

When sharing externally:

- You need to understand the nature of the information in order to assess whether it is appropriate to share with the intended external parties and handle it in accordance with the Bank's policies and obligations.
- Information must only be shared externally where there is a valid business need and disclosure complies with the law. In particular, there may be legislative, contractual or other requirements which limit onward disclosure.
- Where there is any doubt, advice must be sought from management and/or Legal Directorate before sharing externally.

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 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 mandatory process** (data protection requirements may also apply).

Anyone in the Bank could receive a written request for recorded information (for example, by letter or email) 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.
- Complete relevant training, when asked to do so (within One Bank Service, navigate to Me **>Learning**).

External communications and engagement

Engagement and how we communicate with external contacts is a core part of achieving our mission. We are open, honest and straightforward in our external engagement. Comments from any of us who work at the Bank can carry great weight.

The Bank's **>External communications and engagement policy** sets out the requirements for Bank staff when communicating and engaging externally, including specific provisions for the handling of media enquiries, social media use, and participation in 'non-core' meetings and initiatives.

The key policy requirements are:

- Alert Press Office to any reactive or proactive media engagement.
- 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.
- 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 communications and engagement policy**. You will 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.
- You must consult your line manager if you are participating in a meeting or initiative with a third party as a representative of the Bank which is not captured through the conflicts of interest policies and not directly related to your role – defined in the policy as 'non-core initiatives'.

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. The information you share on social media can also be used to target you, those you know and the Bank. It is common for criminals and hostile actors to hide behind seemingly legitimate social media profiles, even posing as recruiters or talent agents, so you must be mindful of engaging with someone you do not directly know.

If you use social media, ensure that you are familiar with the requirements in the social media section of the >**Security conduct policy**.

The key requirements are:

- Do not conduct Bank business through your personal social media accounts or their associated communication services (eg WhatsApp, Facebook Messenger and FaceTime).
- Do not comment on social media on matters that are directly within the interests of the Bank, its mission or its core functions (eg monetary policy, interest rates and regulated firms).
- You should be extremely cautious about comments relating to political issues, 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 employment at the Bank 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, including LinkedIn.
- Do not set up any social media accounts to represent the Bank, or any of its functions or departments, unless authorised to do so.
- Never reveal information about systems and technology used at the Bank, your security clearance, or share details of specific work responsibilities (eg projects you are working on) as this could compromise the Bank's security arrangements.
- Do not post pictures or videos of the interior of any Bank premises externally unless you have explicit permission from Press Office, clearance from Security and a clear business justification, see Being safe and secure. Take care that confidential information is not in view and cannot be overheard while video-conferencing and recording.
- Report to the Investigations and Monitoring Team if you are approached by or have engaged with a suspicious person via your social media.

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 receive indications or speak directly with individuals who allege misconduct (such as fraud, dishonesty, or market

abuse). Equally, these contacts may allege misconduct by third parties. We should report such matters promptly and in the correct manner.

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

If you have been contacted by an external whistleblower or have received evidence or indications of external misconduct in the financial sector, then please adhere to the following information:

- External whistleblowers should be re-directed to the >**Intelligence and Whistleblowing (IAWB) Team** in the first instance.[5]
- If it is not possible to redirect an external whistleblower, then as much detail as possible should be captured (contact details in particular) and passed to IAWB so they can follow up appropriately.
- If you have any doubt as to whether you should treat a contact as a whistleblower or hold whistleblowing related information, please speak to IAWB.
- No further discussion or dissemination of the information should be made. This includes with the firm itself, regulatory counterparts or members within your own team. It is imperative that the 'need to know' principle is applied at all times.
- 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. 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.
- If you have received external whistleblowing information via email, then please forward to **whistleblowing@bankofengland.co.uk** and delete the original email after IAWB have acknowledged receipt. Your HoD, Director or Executive Director will also advise you on how to manage the relationship with the relevant person or firm thereafter.

Information on how we can confidentially raise serious concerns about malpractice or misconduct that affects others or the Bank as a whole, can be found in the internal whistleblowing, '**Speaking up' policy**.

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 have a collective responsibility to maintain the confidentiality, integrity and availability of the information we generate and use, as set out in the **>Governor's Security Charter**.

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 Security Classification Scheme Standard**.

The key requirements include:

- Having a valid business reason to access Bank IT equipment, services, software and information.
- Appropriately classifying all Bank information according to its sensitivity and selecting the right handling caveat (for example, OFFICIAL-BLUE, OFFICIAL-GREEN etc), in line with the Information Security Classification Scheme and handling guidance.
- Use an Insider List to manage access to OFFICIAL-RED information. Follow the **>Insider List standard** and supporting guidance to find out how to set one up correctly.

- Complete relevant training when asked to do so (within One Bank Service, navigate to Me **>Learning**).

The way we handle information, electronically verbally 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 and internal and external information sharing).

The loss or compromise of Bank information can occur in many forms – physically (where we lose papers or a notebook), verbally (conversations overheard in public or within Bank premises), electronically (emails sent to the wrong recipient or information uploaded to an unapproved Artificial Intelligence solution) or via a third party (where a supplier of ours has suffered a data breach).

It is important to follow the **>Data loss reporting process** as soon as you realise information has been lost. The sooner we know about a data loss, the quicker we can take steps to protect the Bank's information.

If you need to take any OFFICIAL-GREEN and/or OFFICIAL-AMBER papers out of the Bank, you should ensure the papers are logged centrally in the appropriate **>form**. OFFICIAL-RED (and above) information must not be taken off Bank premises.

OFFICIAL-GREEN and OFFICIAL-AMBER papers taken off Bank premises must be returned or securely destroyed promptly when no longer needed.

Privacy and data protection

We all have a responsibility to help ensure that the Bank complies with the principles and requirements for handling personal data as set out in privacy and data protections laws.

Personal data means any information from which a living individual can be identified whether directly from the information itself (eg a name, online identifier and location data) or indirectly when combined with 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**. 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;
- 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);
- referring information rights requests from individuals (staff and non-staff) to **data-protection@bankofengland.co.uk** as soon as possible; this includes subject access requests, complaints/concerns or requests for information about how the Bank handles personal data;
- reporting incidents, or suspected incidents, involving personal data loss as soon as possible to your line manager and HoD; follow the **>Data loss reporting process**;
- consulting **Privacy** if your role involves changing the way we collect or handle personal data; and
- completing relevant training, when required to do so (within One Bank Service, navigate to Me **>Learning**).

Using email

We heavily rely on email to communicate with each other and the outside world. While it enables us to do our jobs, it is also the most common medium through which data loss and cyber incidents occur. Although there are technology safeguards in place, the only way to avoid mistakes – such as sending information to the wrong person – is to take extra care when sending emails; double-checking the recipient, attachments and classification and reading and appropriately responding to any warning prompts.

When you are sending emails, remember:

- Do not send Bank information via email unless there is a business justification, you have approval from the asset owner,[6] the email is classified appropriately and sent to a trusted recipient.

- You must not send information that you've created, received, handled or processed as part of your work for the Bank to a personal email address. The **>Security conduct policy** sets out the very limited exceptions which apply (and how to classify the email), such as when you are sending information about yourself to a personal email address eg P60, medical records, your contract of employment or where information is already in the public domain.
- Do not under-classify Bank information in order to bypass security controls. This includes misclassifying Bank information in order to send it to a personal email address (see above).
- Report suspicious emails or attachments immediately by using the Report Phishing button in Outlook, as these could be phishing attempts. Be aware of emails from people you don't know, especially if they come with links or attachments, or from people you do know that ask you to do something unusual.

You can find out more about **>phishing** and how best to protect yourself.

Using Bank IT and other resources

As we work with IT on a daily basis, we need to follow these key requirements which are even more important when working away from the office:

- Ensure that you only conduct Bank business using Bank authorised devices or on Bank-authorised systems and platforms.
- Ensure that your communications and all activity while using IT equipment are appropriate and secure.
- Have complex passwords and do not share, display or reuse them.
- Do not alter the configuration or security settings on Bank IT equipment, or install or use unauthorised applications or software.
- Keep your devices up-to-date with security patches and software updates when prompted by Technology. Shutting down at the end of the day, and logging in correctly applies some of these updates automatically.
- Do not engage in testing the security of Bank IT equipment, systems and software without approval from the Cyber Security Division.
- Do not store information locally on your Bank machine (eg desktop) unless temporarily to support offline working or if local area policies/procedures permit it.

Regular personal use of Bank IT resources and equipment is not permitted. In certain circumstances, occasional and very limited personal use is permitted; however, it must not conflict with our work or compromise the security of the Bank. Occasional and very limited personal use does not extend to using Bank IT to run an external business. Colleagues are expected to display reasonable and professional conduct at all times. If you have a Bank-owned mobile device, please ensure you are familiar with additional requirements in the **>Personal usage guidance**.

Using Bank IT for audio-visual calls

Your communications and activity while using Bank IT equipment must be appropriate and secure. All calls and any information you share via these mediums must be protected, particularly when it includes external participants.

Key requirements include:

- Exercise caution when participating in telephone calls and video conference calls in public spaces, and at home if the nature of the conversation is sensitive. Do not engage in OFFICIAL-AMBER (and above) conversations in public places or where you can be overheard. You should disable smart voice assistants like Siri and Alexa.
- Be aware of potentially sensitive conversations happening around you and of any sensitive information appearing in the background when taking audio or video calls at Bank sites. Use the background features on Microsoft Teams for privacy.
- Use Microsoft Teams or Equinox to set up meetings organised by the Bank. Other communication platforms (such as Zoom, Webex and Go To meeting) can be used and accessed from Bank devices if attending an externally organised event. You must understand the security risks and adhere to precautions detailed in the **>Security conduct policy**.

To find out more on how to use Bank IT safely and securely, please see the **>Security conduct policy**, particularly the section on ‘Use of Bank IT equipment’ and ‘Using audio and video conferencing facilities for Bank business’. This includes a **>Monitoring notice**, which sets out the extent to which the Bank is monitoring use of its equipment.

Safety and security at the Bank's premises

The Bank's premises are a safe and secure environment, however we must all remain alert to matters that look out of place or may indicate a security risk. Immediate concerns must be reported to the Security Control Room. Health and Safety concerns can be reported via Facilities Online or to the Health and Safety team.

You must follow these requirements to ensure the Bank's assets remain safe and secure:

- Display your security pass when entering Bank premises and continue to wear it while on site.
- Remove your security pass as you leave the premises – including when travelling between Bank premises.
- Do not share your security pass with other Bank staff or visitors, either to access or move around Bank premises, or for printing and catering.
- Do not allow colleagues or visitors to enter restricted areas unless they have a valid business reason for being there, even if they present a staff pass. You should feel empowered to challenge another member of staff who you find in a restricted area who you believe should not be there.
- If you invite visitors to the Bank – follow the **>Requirements for visitors**. In particular, ensure your visitors are registered with reception ahead of time, and can provide acceptable ID upon arrival to be allowed access. Also, ensure they are escorted at all times by a member of staff when on Bank premises. You should feel empowered to challenge any unescorted visitor, and politely escort them to where they should be. If your visitor takes an unauthorised picture or film of Bank internal premises, you must ask them to delete this from their device.
- Maintain a clear desk overnight, locking papers and laptops away and removing personal items – if you are the last one to leave your working space, you should ensure items have not been left out. During the day when leaving your desk for any period of time, lock your computer screen and secure Bank information.
- You must comply with the restrictions on photography and filming within any Bank premises as set out in the **>Security conduct policy** (see also the 'Use of social media' section to understand more about posting photos online).
- Ensure you understand **>Health and safety policy**, and complete relevant training when asked to do so (within One Bank Service, navigate to Me **>Learning**).

We help protect ourselves, colleagues and visitors by reporting promptly any issues or concerns about safety or security.

Safety and security outside the Bank's premises

Safety and security are also a priority whenever we are working away from Bank premises.

If you are 'working away from Bank premises', eg at home, in transit or abroad, the **>Security conduct policy** sets out the steps you must take in order to help maintain physical and information security.

Key requirements include:

- Exercise caution when participating in telephone calls and video conference calls in public spaces, and at home if the nature of the conversation is sensitive. Do not engage in sensitive conversations (OFFICIAL-AMBER and above) in places where you can be overheard.
- Protect your laptop with a privacy screen if using in public spaces, such as on trains. If you work as you travel, your Bank equipment and information must remain secure.
- Use the Bank's self-reporting **>form** to log any OFFICIAL-GREEN and OFFICIAL-AMBER papers, notebooks or handwritten notes taken off-site overnight. OFFICIAL-RED information cannot be taken off Bank premises and additional restrictions will apply in areas of heightened sensitivity (eg committees, resolution and stress testing). Papers taken off Bank premises must be returned or securely destroyed promptly.
- Requirements for secure storage, transport and disposal of Bank information can be found in the **>Security conduct policy**.

If you intend to work abroad:

- **Temporarily and for personal reasons** – you must comply with the **>Working from abroad policy**. This includes not taking any Bank IT equipment (laptop, ipad or phone) when visiting (or transiting through) countries highlighted listed in Appendix One of the policy. Under no circumstances can Bank IT equipment be taken to environments on the high cyber threat list.
- **If the Bank has asked you to travel to conduct Bank business** – you must comply with the 'Business Travel' section of the **>Security conduct policy**. This

means you have to book through the appropriate channels and follow the advice of Travel Security for travel to any high cyber or physical threat environments.

Safeguarding against money laundering, terrorist financing and proliferation financing[7] 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 or proliferation financing activity or are not complying with financial sanctions.

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, proliferation financing or financial sanction breaches may occur or have occurred.
- Complete relevant training, when asked to do so (within One Bank Service, navigate to Me **>Learning**).

If you are involved in the Bank's financial operations, then you must be aware of relevant anti-financial crime controls and support their effective operation. A small number of teams around the Bank may need to consider the impact of US sanctions and if you receive notification that you are a relevant line manager then you must seek advice from the Financial Crime Team if anyone in your team is a US person. See the **>Anti-money laundering, counter terrorist financing, proliferation financing and financial sanctions compliance policy**.

Safeguarding against tax evasion

The Bank has zero tolerance for tax evasion, and we safeguard against the risk of facilitating any such activity. If you have any concerns, raise these with the **>MLRO**.

You must complete relevant training, when asked to do so (within One Bank Service, navigate to Me **>Learning**).

Creating a diverse, inclusive and empowering culture

We fully embrace diversity, equity and inclusion and the benefits they bring. To achieve this, we need everyone to help create an inclusive culture at work; avoid non-inclusive behaviours; speak out when you observe non-inclusive behaviour; and be open to feedback about your own behaviour.

Building a diverse and inclusive Bank in which everyone feels they belong is a strategic priority for the Bank. The current global context presents both challenges and opportunities, and the Bank needs to be human, humble and in step with the changing world to respond effectively. We need leaders, managers and staff who embody this ambition, and a truly inclusive culture to enable all colleagues, whatever their background and ability, to reach their full potential. We also seek to ensure that colleagues are supported in managing their time between work and personal life, to enable them to thrive at the Bank. We do this because it is the ethically right thing to do and because it will make us even more effective as an organisation, now and for the future.

Diversity, equity and inclusion strategy

The Diversity, equity and inclusion strategy is evolving and is an important part of delivering the culture we need and in supporting Strategic Priority Six (SP6), ‘Build a diverse and inclusive Bank’. This creates a framework to bring together various strands of work which aim to:

- advance the development of an inclusive culture;
- adapt our culture and behaviours to support new ways of working, learning from internal and external experience;
- transform our leadership capability to support our human and humble ambition and cultural vision; and
- develop a more diverse workforce and implement the Court Review’s recommendations.

There are Directorate, Deputy Governorship and Bank-wide inclusion initiatives and you can learn more about the Bank’s approach to inclusion by speaking to the Culture, Diversity, Equity and Inclusion Division, or your area’s Diversity and Inclusion lead, as outlined in **>Inclusion across the Bank**.

During attestation, each year, we ask you to complete the Personal Data Review (PDR) in One Bank Service to ensure your personal information, including contact details, are correct.

As part of this, we ask you to complete the ‘Demographic Info’ and ‘Disability and long-term health conditions’ sections of the PDR. Sharing your personal information with us helps ensure that we support all colleagues effectively, allowing us to build a better picture of the people who work for the Bank and so target our activity effectively. Information shared with the Bank in the ‘Demographic Info’ and ‘Disability and long-term health conditions’ sections in One Bank Service cannot be viewed by your manager(s).

Declared diversity characteristics are used to produce metrics across the employee lifecycle and for a range of activities to enable the Bank to monitor targets and pursue its diversity and inclusion objectives. Whenever possible, this is done without identifying individuals. For small populations, where it may be possible to identify an individual, access to this type of personal data is strictly limited with defined access controls. If you would prefer not to share this information at any stage, you can select ‘Prefer not to say’.

Discrimination, bullying and harassment

> The Bank does not tolerate discrimination, harassment, bullying and victimisation. All employees have a responsibility to help ensure everyone they work with and those visiting the Bank are treated with dignity and respect and to take steps to prevent harassment, bullying, victimisation and/or retaliation.

The impact of your actions matters as much as your intent. The Bank may consider an individual’s actions and behaviour as bullying or harassment, even if this was not the intention.

In line with **Our Bank Behaviours**, we expect all staff to raise any concerns about possible bullying, harassment, victimisation, or any other inappropriate behaviours as soon as possible.

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 and the Employee Relations Team under the **>Diversity policy** or the **>Anti-bullying and harassment policy**.

We recruit, hire, develop, promote, manage and provide conditions of employment without unlawful regard to age; disability; gender reassignment;[8] marriage and civil partnership; pregnancy and maternity; race; religion or belief; sex; sexual orientation. We are all personally responsible for the avoidance of unfair discrimination under the Equality Act 2010.

Active by-standing

Active by-standing is taking action to stop the harm when a colleague is experiencing microaggression, harassment, bullying or other harmful or inappropriate behaviour that takes place in your presence. We strongly encourage appropriate active by-standing which helps to advance our diversity, equity and inclusion goals. We support colleagues who intervene. It is illegal to suffer adverse treatment from leaders, managers and colleagues because of your active bystander intervention. Please contact the Employee Relations Team if you need support.

Speaking up (internal whistleblowing)

The **Speaking up policy** (internal whistleblowing) sets out how you can confidentially raise serious concerns about malpractice or misconduct.

We need this policy because when things are going wrong in an organisation the signs are often there for everyone to see. Usually they are spotted, reported up the management chain and acted upon. But sometimes they are not. Management may not listen. Staff may not feel confident enough to raise a concern. They may see management as the problem.

At the Bank, we want to ensure that this does not happen and that all voices are heard. Therefore, if you have a serious concern about malpractice or misconduct that affects others or the Bank as a whole – such as possible fraud, criminality, breach of a legal obligation, environmental damage, or a danger to the Bank and its staff – it is vital that you report it so that it can be addressed. This is how you can help protect other staff and the Bank.

Even if you are not completely sure if your concern is serious, but you feel that something is not quite right, it is important that you Speak up. If your concern is not covered by this policy, we can redirect your concern to the right people.

Speaking up is an integral part of the Bank's culture. We are committed to fostering an environment where individuals feel safe and have the confidence to raise serious concerns without fear of retaliation or reprisal.

Please raise such concerns via the **>Speaking up (internal whistleblowing)** arrangements, whether via line management, Secretary's Department, a Speaking up nominated representative, or a confidential external helpline provided by Vita Health Group. Protect, the UK whistleblowing charity, can provide confidential advice to people thinking of Speaking up.

Contact details for all the above are contained in the Speaking up policy.

To those who Speak up, we undertake that:

- You will not lose your job or suffer any other penalty as a result of Speaking up. It does not matter if you are mistaken. We do not tolerate any victimisation or harassment of those who speak up.
- We treat Speaking up matters sensitively. Anonymous disclosures can be more difficult to investigate, so we do not encourage them. If you 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 further action.
- We will investigate your concern thoroughly and impartially as we determine is appropriate.
- We will update you as appropriate once our investigation is completed.
- However, maliciously reporting matters that you know to be false may result in disciplinary action.

Mandatory courses we need to complete

We must all keep up-to-date with mandatory training and complete (and repeat) courses when asked to do so. All courses are available in One Bank Service, navigate to Me **>Learning**.

The following mandatory e-learning courses must be completed by ALL new joiners within 30 days of joining the Bank:

- Emergency Procedures (2023).
- Security Annual e-learning (2023).
- Data Protection e-learning (2023).
- Freedom of Information.
- Records and Information Management at the Bank of England (2022).
- FileSite.
- Diversity, Equity and Inclusion at the Bank of England (for new joiners from June 2022).

In addition, all existing colleagues will be asked to repeat the above courses (apart from the FileSite course) at periodic intervals.

Anti-money laundering training

The following areas of the Bank must complete the first module of anti-money laundering e-learning:

Deputy Governorship	Division	Teams
Markets, Banking, Payments and Resolution	Central Banking Operations	• Custody, Settlement and Liquidity
	Customer Banking	• Banking Operations • Customer Banking Division
	Market Services	• Payment Systems and Communications • Policy, Regulatory Affairs and Governance • Participant Performance and Assurance • Payment Systems Risk • Policy Implementation • MSD Border Payments Policy • PRG Policy and Analysis • RTGS Chaps Board and Committee Secretariat • Payment Systems and Communications Change
	MBPR COO	• Business Planning • Operational Risk • MBPR Projects Division • MBPR Strategic Change and Operations • ISO 20022 Programme
	Sterling Markets Division	• Sterling Operations • Operational Policy • SMD Benchmarks and Policy Strategy
	Foreign Exchange (FX) Division	• Reserves Management • Policy • FX and MM

Deputy Governorship	Division	Teams
	Market Intelligence and Analytics (MIAD)	• MIAD Market Intelligence Delivery Team • MIAD Structural Analysis Team • MIAD Market Policy Analysis Team
	Financial Risk Management Division	• Collateral Risk • Credit Risk • Traded Risk • Quantitative Risk Analytics • Climate change
	Future balance sheet including: stablecoin	• Governance of the Balance Sheet • Overall Asset Portfolio • Future Monetary Operating Framework • Projects and Programmes Delivery • Stablecoin/mitigants • FS buy/sell Tool • FS NBFI Repo Tool • Enabling CBDC Design and Evaluation
	Middle Office	• Pricing Policy and Valuation • Collateral and Counterparty Operations • Operational and Financial Control • EDM Support Team

Deputy Governorship	Division	Teams
	Resolution	• Domestic Resolvability • International Resolvability • Policy • Office Management • FSBO • Resolvability Assessment Framework • Heightened Contingency Framework
Monetary Policy	Notes Operations	• Banknote Operations • Banknote Supply Management • Banknote Security and Design
	Future of money	• Banknote Analysis, Strategy and Engagement • Wholesale Policy and Supervision
	Centre for Central Banking Studies (CCBS)	• CCBS • DFID
	Monetary Analysis	• Structural Economics • Monetary Policy Outlook • Current Economic Conditions • External Engagement • Monetary and Financial Conditions • COO • External MPC Unit • MA General • Monetary Analysis and Chief Economist ED Office • Agencies • Monetary Analysis Strategic Priorities

Deputy Governorship	Division	Teams
Financial Stability	Financial Market Infrastructure Service (includes FMI supervision)	• Post Trade Policy • Innovation and Payments Policy • Evidence Based Analytics Supervision • Financial Market Infrastructure Strategic Priorities • FMI Executive Directors Office Division • FMI Payments, Settlements and Innovation Supervision Division
	Financial Stability Strategy and Risk (FSSR)	• Stress Testing Strategy • Capital Markets • Macro-Financial Risk • Macroprudential Strategy and Support • Banks Resilience • Emerging Risks and Special Projects • Climate Hub Division • FS Strategy and Risk Strategic Priorities • FS Strategy and Projects Division (FSSP) • FPC • FS COOD FSSR ED’s Office
	International (also reports into Monetary Policy)	• International Surveillance • Global Analysis • Policy and Strategy • ED Office International • International Strategic Priorities
	Central Bank Digital Currency (CBDC)/Fintech	• CBDC Division • BIS and Fintech Division • CBDC Strategic Priorities

Deputy Governorship	Division	Teams
Governors Direct Reports	Governor's office	• Deputy Governor for Markets and Banking • Deputy Governor for Financial Stability • Deputy Governor for Monetary Policy • Governor's Office • Chief Operating Officer
	Legal and Legal – Whistleblowing	• Central Banking • Financial Stability • Enforcement and Litigation • International and Domestic Reform • Insurance and Deposit Takers • Strategy and Operations Unit • General Counsel's Office
	Communications	• Strategic Communications • Internal Communications • Content Delivery • Content Creation General • Information Access • Parliamentary Affairs • Outreach and Education • Press Office • ED Comms
	Internal Audit	• Monetary Stability and Operations • Prudential Regulation Authority • Technology • Government, Central Services, and Internal Audit Processes
	Risk	• Enterprise Risk and Resilience • Compliance • Financial Risk and Resilience

Deputy Governorship	Division	Teams
	Secretary's, includes Personnel and National Security	• Personnel Security • National Security Unit • Court Secretariat • Executive Secretariat • Conflicts • Archive • Records Management • Information Centre • Investigations • Secretary's Office • Non-Executive Directors • Independent Evaluation Office
	Finance and Performance	• Finance Transformation • Financial Control and Reporting • Planning and Reporting • Business Partnering • Finance ED Office • Corporate Portfolio Office • Finance Operations Team
Prudential Regulation Authority (PRA)	PRA	• Risk and Operations • Supervisory Risk Specialists • Insurance Supervision • Authorisations, RegTech and International Supervision • UK Deposit Takers • Prudential Policy • PRA Central

Deputy Governorship	Division	Teams
Chief Operating Officer	People and Culture	• Culture, Diversity, Equity and Inclusion • Employee Relations • Reward • Talent Acquisition and Development • People Operations • People ED Office • Secondments and Study
	Technology	• Applications and Product Engineering • RTGS
	Shared Services: Property, procurement and security business services, strategy and change	• Property • Security • Procurement • Central Operations Project • Corporate Services Operations • Central Operations Executive Director
External Court NEDs	External Court NEDS	External Court NEDs
External Policy Committee Members	External Policy Committee Members	External Policy Committee Members

Staff in Markets and Banking, and those in Internal Audit looking after Markets and Banking, are also required to complete the second module of anti-money laundering e-learning.

If your work involves the physical process of exchanging bank notes you are required to complete the third module of anti-money laundering e-learning. The Financial Crime Team will be in touch directly to let you know if this applies.

Tax evasion course

The following areas of the Bank must also complete the course ‘Criminal facilitation of tax evasion 2023’:

- Finance and Performance Directorate.
- Technology Directorate.
- People Directorate:
  - Talent Acquisition and Development Division;
  - Secondments and Study Division;
  - People ED Office; and
  - People Operations Division.
- Central Operations Directorate:
  - Corporate Services Operations Division;
  - Central Operations Executive Division;
  - Central Operations Projects Division;
  - Procurement Division;
  - Security Division: only Scale F and above; and
  - Property Division: PPSD HoD and Business Management, PPSD Projects, Capital Works and Estate, Health, Safety and Environmental, Events and Services: only Scale F and above and AV Team.
- Payments:
  - RTGS Renewal Finance Team.

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

Conflict of interest checklist	Page number
Disclose and keep up-to-date:	
Personal relationships	See **here**
Disclose to the Secretary, Deputy Secretary or Conflicts Team:	
Discussions about employment with a Bank regulated firm, a significant dealing counterparty of the Bank or firm that you have contact with as a supplier	See **here**
Financial relationships	See **here**
Community or charity roles with formal responsibilities, including becoming a trustee	See **here**
Involvement in political activities	See **here**
Seek approval before:	
Making a personal financial transaction covered by the pre-approval requirements	See **here**
Taking up a company directorship	See **here**
Taking up additional employment	See **here**
Putting yourself forward for selection for local or national elected office	See **here**
If offered entertainment and gifts:	
Discuss with senior management if in doubt about what you can accept	See **here**
Report any entertainment and gifts received	See **here**

Other disclosures/permissions	Page number
If your personal circumstances change materially:	
Make the Security Vetting Team aware	See **here**
If you want to take part in a media discussion or speak at an event where the media is present:	
Seek the Bank's Press Office approval	See **here**
If you want to take OFFICIAL-GREEN or OFFICIAL-AMBER papers off-site overnight:	
Follow the requirements in the **>Security conduct policy** to log these	See **here**
If you want to take a photograph, video or recording the Bank:	
You need permission under the **>Security conduct policy**	See **here**

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.

Policy	Report
Breaches of Our Code or other Bank internal policies	Report direct to the Compliance Division via **AskCompliance@bankofengland.co.uk**
Security incidents/emergencies	Report to the Security Control Room For incidents of a technical nature, report to the Technology Service Desk For security concerns/queries **askcybersecurity@bankofengland.co.uk**
Bullying, discrimination or harassment	Discuss with Employee Relations Team Log an AskHR call in One Bank Service
Data protection breach or any loss of Bank information or devices	Report to your line manager and HoD. Follow the **>Data loss reporting process** Outside working hours telephone the Security Control Room or the Technology Service Desk
Freedom of Information request and Subject Access request	Forward to the Information Access Team **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 Employee Relations Team Log an AskHR call in One Bank Service (NB Grievances are governed by the Staff Handbook, not Our Code)

Policy	Report
Speaking up (internal whistleblowing: serious concerns about disregard of internal Bank policies, a risk to the Bank, a possible fraud, misconduct or malpractice)	Discuss with your line manager, nominated representatives listed in the Speaking up policy or Speak up Team in Secretary's as listed in the policy
Escalation of external misconduct concerns	Your HoD, Director or the Bank's Intelligence and Whistleblowing Team via **whistleblowing@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 **AskCompliance@bankofengland.co.uk**

Contact the relevant policy owner/expert, as follows:

Policy	Policy owner/expert
Breach management policy	The Compliance Department **AskCompliance@bankofengland.co.uk**
Conflicts of interest policies (personal relationships, financial relationships, personal financial transactions, directorships, community and charity roles, political activities) Entertainment and gifts policy; Secrecy declaration; and Speak up policy (internal whistleblowing)	The Secretary's Department Conflicts Team **AskConflictsAdvice@bankofengland.co.uk**
External Whistleblowing Policy Owner: Intelligence and Whistleblowing Team (IAWB)	**whistleblowing@bankofengland.co.uk**
Restricted duties policy and Other employment policy (co-owned with the Secretary's Department) Anti-bullying and harassment policy; Inclusion and Working from abroad policy	Employee Relations Team Log an AskHR call in One Bank Service

Policy	Policy owner/expert
Records management policy; Creating Records of Meetings, Committees and Calls policy; Audio and audio-visual recordings of meetings policy; and Internal and external information sharing policy	The Secretary's Department – Records Management Team **BankRecordsManagementTeam@bankofengland.co.uk**
Security conduct policy Privacy and data protection conduct policy Security Vetting Social media	Cyber Security **AskCyberSecurity@bankofengland.co.uk** Privacy **AskPrivacy@bankofengland.co.uk** Security Vetting **PPSD-Vetting@bankofengland.co.uk** **ASKCyberSecurity@bankofengland.co.uk**
Health and Safety policy	Health and Safety **HealthandSafety@bankofengland.co.uk**
Freedom of Information Subject Access Request	Information Access Team **Information-access@bankofengland.co.uk**
Data Management and Analytics	Data Management team **DAHelpDesk@bankofengland.co.uk**
External communications and engagement policy	Press office **Press@bankofengland.co.uk**
Anti-money laundering, counter terrorist financing and financial sanctions compliance policy	Money laundering, Operational Risk and Compliance, Markets and Banking COOD **MLRO@bankofengland.co.uk**
Procurement policy	PPSD, Procurement **Askprocurement@bankofengland.co.uk**
Safeguarding against tax evasion	Finance Division, ED Office **Finance-EDOffice@bankofengland.co.uk**

Policy	Policy owner/expert
Travel and expenses policy; non-travel related expenses policy	Finance Division, Expenses **Finance-Expenses@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.

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), line management, the Compliance Division and Internal Audit. It may also be necessary for Our Code related information to be made available to the People Directorate (formerly known as People and Culture Directorate), the Security Vetting Team, the Legal Directorate 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.

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 **>How we use staff data notice** or visit **>Privacy and the Bank of England**.

January 2024

---

1. A breach is a failure to act with integrity, in accordance with Our Code and/or the Staff Handbook, or a failure to comply with a Bank policy.
2. Also known as the Nolan Principles: selflessness, integrity, objectivity, accountability, openness, honesty and leadership. See **>GOV.UK**, The Seven Principles of Public Life.
3. As defined in the publicly available MPC and FPC Communications Codes.
4. The Bank offers a range of services to support colleagues' physical and mental wellbeing, including for colleagues facing financial difficulty.
5. External whistleblowing forms part of a wider portfolio of intelligence and financial-crime related services managed by the IAWB team. The team currently comprises three members of staff, overseen by a Deputy Head of Legal within the Legal Directorate's Enforcement and Litigations Division. In addition to leading day-to-day on, and managing all aspects of, external whistleblowing in relation to regulated firms, the team manages the Bank's relationship with whistleblowers, provides technical specialist support, including learning and development for PRA Supervisors, deals with law enforcement agency and Bank Confidential enquiries, works with the rest of the Legal Directorate to assess what further steps may be needed on cases and participates in supervisory meetings with firms.
6. Asset owner: a member of staff that is either the author or creator of an asset. If not known or unclear, this may be the relevant HoD or higher.
7. Proliferation financing is broadly defined in **regulation 16A(9) of the Money Laundering Regulations 2017** as 'the act of providing funds or financial services for use, in whole or in part, in the manufacture, acquisition, development, export, trans-shipment, brokering, transport, transfer, stockpiling of, or otherwise in connection with the possession or use of, chemical, biological, radiological or nuclear weapons, including the provision of funds or financial services in connection with the means of delivery of such weapons and other CBRN-related goods and technology, in contravention of a relevant financial sanctions obligation'.
8. Protected characteristics have been taken from the Equality Act 2010. The Bank treats gender reassignment, gender affirmation and gender identity as within equal scope for protection, regardless of medical transition status.