Anti-Bribery and Corruption Guidance

Associated Group Risk Category: Legal Compliance

Associated Standard: Anti-Bribery and Corruption

Applicability: This guidance applies to everyone working for, or on behalf of, BT. It is particularly relevant to managers working in customer-facing roles, procurement, sales, marketing, corporate affairs, bid and contract management.

Objective of this document: This Guidance document is to help you make informed decisions.

Being trusted: our code and BT's position on Facilitation Payments, Blackmail and Extortion, Public Officials and Political Donations are mandatory. You must ensure that you read, understand and comply with our Anti-Bribery and Corruption Standard

Contents **Page**

1 Facilitation payments

1.1 BT's position on facilitation payments

At BT, we take a zero-tolerance approach to bribery and corruption. We are committed to acting professionally, fairly and with integrity in all our business dealings and relationships wherever we operate.

BT prohibits facilitation payments. We will not make them and we will not allow others to make them on our behalf.

1.2 What are facilitation payments or "kickbacks"?

Facilitation payments, also known as "grease payments", are typically small, unofficial payments made to secure or expedite a routine or necessary government action by a government official, when we have already paid for, or are entitled to, that action. The payment is typically not intended to influence the outcome of the official's action but the pace of the action. A typical example might be 'inspection fees' for clearance of imported equipment through customs. This does not include fees required to be made by law, such as taxes.

"Kickbacks" are typically payments made in return for a business favour or advantage.

Facilitation payments and "kickbacks" are both a type of bribe and are illegal in many countries, including the UK.

1.3 Guidance of facilitation payments

This Guidance contains steps to help you make BT less vulnerable to demands for facilitation payments and "kickbacks".

If you work in an area where a facilitation payment may be requested, advance planning will help to mitigate the risk of this.

The safety of all of our people is paramount. You should never refuse to make a payment if you, or someone connected to you, is faced with a threat, or fear of, violence or loss of liberty.

1.3.1 Research – preparation is key

1. Research local laws in advance; understanding the official requirements will make it easier to identify and resist a request for payment. If you're unsure as to what may be properly payable fees and what may actually be a disguised request for a facilitation payment, seek advice from the Ethics and Compliance Team. Always seek approval before making a payment, except if you, or someone connected to you, is faced with a threat, or fear of, violence or loss of liberty.
2. Research what authorisations or permits are needed well in advance, in cooperation with any relevant intermediary. If possible, get official written confirmation that all documents are in order and have this to hand should a facilitation payment be requested.
3. Build in the necessary time required to get through the administrative formalities well in advance so that time pressure is less likely to be an issue.

1.3.2 Resistance – how to respond to a request for a facilitation payment

Only if it feels safe to do so:

1. Question the legitimacy of the request and politely refuse to pay. Even if your refusal to pay the bribe is accepted, report the request to your BT Legal representative and to Speak Up.
2. Explain that you don't believe you need to make the requested payment as all of your papers are in order (use your research on local laws to support this).
3. If they persist, explain that your company prohibits such payments and that you are required to report the incident to your company who will report the incident to the authorities.
4. If appropriate, ask to speak to a more senior official.
5. If the request to speak to a more senior official is refused or the official is unhelpful, explain that your company will be forced to make a formal complaint.
6. **You should never refuse to make a payment if you, or someone connected to you, is faced with a threat, or fear of, violence or loss of liberty.** Only in this circumstance should you make a payment, but if it is safe to do so, try to:
   a) Negotiate the minimum amount.
   b) Try to avoid making a payment in cash.
   c) Obtain a receipt for any payment that you make so these can be accounted for to help demonstrate the legitimacy of the payment.

1.3.3 Recording – as soon as possible after the situation

1. Keep a detailed record of all requests for payment and any payment which you have had to make (including witness evidence where possible).
2. If possible, record the name of the individual requesting the payment and any other details to identify those involved.

1.3.4 Reporting

1. As soon as it is safe to do so, report the payment to your manager explaining why you had to pay it.
2. Record the payment on the expenses system with a clear explanation of its purpose.
3. You must report the incident to your BT Legal representative and to Speak Up.

All incidents will be considered by the Director of Ethics and Compliance (or their delegate). This will help BT in its efforts to reduce the risk of reoccurrence.

1.3.5 FAQs

Q: I'm suffering a delay in customs despite all the required papers being in order. It seems that a small tip would make the process quicker. Can I give one?

A: No, such a payment would be a facilitation payment and such payments are prohibited by BT. They are also illegal under the UK Bribery Act 2010 which has global reach and, like similar laws such as the US Foreign Corrupt Practices Act, apply wherever we do business.

Q: I am having difficulties importing kit and equipment which is needed by the customer at their location. The import inspectors are insisting that I pay an "inspection fee" before they will issue a certificate of inspection and clear the goods. Should I make this payment?

A: You must first get confirmation that the fee is legitimate before making any payment as the request from the inspectors could be a request for a bribe. If it is not legitimate, you must not pay this fee. If in doubt, please contact the Ethics and Compliance Team.

Q: I am working with a local agent to help set up a project in-country. They are working with the authorities to obtain the necessary permits on BT's behalf. They've asked for an advance payment to speed things up. Should I make the payment?

A: No. Requests for advance payments are themselves a red flag for corrupt behaviour and the suggestion that this would "speed things up" is an indication that the payment could be a bribe. BT is liable under the UK Bribery Act for the actions of third parties working on our behalf anywhere in the world, such as agents and consultants, and we must be vigilant to ensure they do not make such payments. If in doubt, please contact the Ethics and Compliance Team.

Q: What if I fear for my safety when asked for a facilitation payment?
A: The safety of our people is paramount. If you fear for your safety, or the safety of someone connected to you, then make the payment. Please contact Speak Up to report the incident as soon as it is safe to do so.

Q: What shall I do if I suspect that someone has made a facilitation payment?

A: You must report this to Speak Up when it is safe to do so.

2 Blackmail and Extortion

2.1 BT's position on blackmail and extortion

We do not tolerate anyone working for, or on behalf of, BT making or receiving threats of blackmail or acts of extortion. Blackmail and extortion are criminal acts and punishable by imprisonment. Where anyone acting for or on behalf of BT is found to have committed an act of blackmail or extortion, this will result in dismissal or termination of the supplier contract.

The purpose of this section is to help you respond appropriately if faced with blackmail or extortion.

2.2 What are blackmail and extortion?

Blackmail and extortion are slightly different.

Blackmail is the term given to acts of attempting to make a gain or encouraging a loss to another through unwarranted demands accompanied by threats or menacing behaviour. This will include, for example, threatening to expose sensitive, embarrassing or incriminating information about an individual if they do not comply with a demand. The threat does not have to be illegal, or even true, for it to be considered blackmail. This will also include exerting pressure to induce someone to act in a particular way or make an unfair decision.

Extortion refers to the act of making a threat of violence, harm or destruction of property to coerce a victim into complying with demands. This includes corrupt officials abusing their position to obtain property, funds or patronage by extortion. A further form of extortion is where unethical businesses charge excessive or exorbitant fees for vital services.

2.3 Risk reduction measures

Here are some simple measures you can take to reduce the risk of another party committing an act of blackmail or extortion:

1. Use electronic communications with external parties;
2. Use legal support when attending meetings with parties that present a higher risk of solicitation;
3. Use systems that reduce face-to-face contact when interacting with government officials or making financial transactions, even when this involves payment of a valid fee. This may include:
   a) E-invoicing;
   b) E-filing of taxes, contributions, licensing;
   c) E-procurement, e-tendering, e-sourcing;
   d) Electronic platforms for interactions or transactions with governments.
4. Where appropriate, taking part in open dialogue with external organisations to promote transparency and the reduction of corruption risk.

2.4 How to respond to blackmail and extortion

This section covers four areas:

I. Where a request for a bribe is made but there is no threat to personal safety;
II. Where a request for a bribe is made and there is a threat to personal safety;
III. Where you are aware or have reasonable grounds to suspect that a colleague is or is at risk of being the subject of blackmail or extortion;
IV. IV. Where you believe that you are a victim of cyber extortion.

In the event that you are subjected to, or become aware of, any of these behaviours you must report this, as detailed below.

2.4.1 A request for a bribe is made but there is no threat to personal safety

Here are two scenarios where this may occur:

1. You are asked for a bribe and the other party tries to coerce you into making the payment by exerting pressure on you and/or the business. For example, you may be told that something happening or not happening is dependent upon payment of money in circumstances where the money is not legitimately due;
2. Someone attempts to blackmail you and they seek to compel you to make a payment or carry out an action in return for not revealing secret or sensitive information about you or someone connected to you. In some locations, corrupt officials may seek to entrap you by deliberately obtaining such information in order to use it to gain business favours or an illicit payment.

Here's what to do if you are confronted with either of these scenarios:

1. Politely refuse to pay the bribe. Even if your refusal to pay the bribe is accepted, all instances need to be reported to your BT Legal Representative and to Speak Up.
2. If you are told that these are legitimate charges, such as a tax, seek confirmation from your BT Legal Representative or, if it relates to customs/imports, from the Director of Ethics and Compliance (or their delegate). Always obtain a receipt for any payments that you make after you have been granted permission to do so.
3. If the individual persists, inform them that your company prohibits payments of bribes and that, if you pay the bribe, you will have to report it to your company, including the details of the individual making the demand. Tell the individual that your company will then report the incident to the individual's employer and the criminal authorities.
4. If the demand is made by a public official, and there are government procedures in place to report the official, then inform the official that these procedures require you to report the request. If the situation is not resolved, ask to speak to a senior official or manager.
5. If the request to speak to a senior official or manager is refused or they are unhelpful, explain that your company will make a formal complaint to the relevant government department or company responsible.

You must always:

a) Keep a detailed record of all requests for such payments (including witness evidence); AND
b) Report any incident, whether payment was made or not, to your BT Legal Representative and to Speak Up.

2.4.2 A request for a bribe is made and there is a threat to personal safety

This is where you are asked for a payment and you feel that your physical safety, security or liberty, or the physical safety, security or liberty of someone connected to you, is at risk. For example, you are told by a local police office to make an illicit payment and if you don't, you will not be allowed to leave the country.

Here's what to do if you are confronted with this scenario:

1. If the personal safety of you or another is endangered by a refusal to pay, then pay the bribe. You must never endanger your safety or that of another. Our security and safety are paramount.
2. Remove yourself from the situation as soon as possible.
3. Seek advice from the 24/7 Security Control Desk immediately.

You must always:

a) Keep a detailed record of all requests for such payments (including witness evidence); AND
b) Report the incident immediately to your BT Legal Representative and to Speak Up.

2.4.3 You believe that you are a victim of cyber extortion

Cyber extortion is the act of cyber-criminals demanding payment through the use of or threat of some form of malicious activity against a victim. There are many different forms of cyber extortion but some of the most common are:

1. Ransomware: In a ransomware attack, the attacker tricks the victim into clicking a link or pop-up ad, opening a corrupted file sent through email or visiting a website. Such actions "activate" the ransomware, which spreads and infects the company's site, computers or the entire network.
2. Distributed denial-of-service (DDoS): In DDoS attacks, attackers deploy a network of infected computer systems to send a flood of internet traffic that can cripple a website, server or system. DDoS attacks are like a traffic jam. Attackers might only stop their DDoS attack after the victim pays up. Sometimes, attackers first send a warning of the DDoS attack and then demand payment to not continue the attack.
3. Email-based cyber extortion: This may be where victims are told that their personal information will be exposed if they don't pay a ransom within a tight deadline.

For all forms of cyber extortion, bitcoin is the most common form of ransom demanded as it's widely believed to be an untraceable method of payment. However, other cryptocurrencies may also be used.

Here's what to do if you are confronted with this scenario:

1. Disconnect the PC/laptop/tablet/mobile believed to be infected from the network immediately; AND
2. Report this to the 24/7 Security Control Desk on **0800 321 999** (UK) or **+44 (0)1 908 641 100** (International).

You must always:

a) Make a record of all events that could be related to cyber extortion;
b) Report the incident immediately to your BT Legal Representative and to Speak Up.

If you are based in or visiting a jurisdiction where there is a high risk of blackmail or extortion, please visit the Security website for further advice and guidance on travel.

3 Public Officials

There are strict rules around how you may engage with public officials.

3.1 What are public officials?

The definition of a public official is wide. A public official includes officials, whether elected or appointed, who hold a legislative, administrative or judicial position of any kind. It also includes any person who performs public functions in any branch of the national, local or municipal government or who exercises a public function for any public agency or public enterprise. This includes:

a) Any official or employee of a government or any department or agency;
b) Elected politicians – this includes political party officials, employees or candidates for political office or unelected representatives such as members of the House of Lords in the UK;
c) Political appointees – this includes people appointed to or employed by a non-departmental public body (for example, Ofcom, the Environment Agency or the Ordnance Survey);
d) An official or agent of a public international organisation, such as the United Nations (UN) or the World Bank;
e) Civil servants and officials in government-run services – this includes administrative and judicial officers and officials in government-run services like the NHS;
f) Officers and employees of government-owned or government-controlled enterprises – this includes health care systems, the BBC and public international organisations like the World Bank;
g) The Police and *other security agencies, such as* customs and border agents;
h) The Armed Forces;
i) Members of a Royal Family and the Head of State;
j) Any private person acting officially on behalf of a government department, agency or a public international organisation such as the UN.

3.2 What is the risk with public officials?

A high degree of risk exists when we interact with public officials because they may be in an actual or perceived position of influence that could affect BT.

3.3 Engaging with public officials

Anti-bribery and corruption laws demand stricter rules around how companies interact with public officials.

Offering, giving or receiving gifts and hospitality to or from public officials carries a higher risk, and may be against the law. You must ensure that all gifts and hospitality above £25 offered, given or received to or from public officials have prior approval from the Director of Ethics and Compliance (or their delegate). This allows the Ethics and Compliance team to review your registration, and where required, mitigations can be put in place beforehand to ensure we comply with all relevant rules.

We don't pay for travel or accommodation as it is may be seen as excessive and it significantly increases risk. You must keep a record of the details of all recipients and add this to your registration. This helps us track across BT if the same individual or organisation is receiving multiple BT invitations, gifts or hospitality.

You should get written confirmation from the public official, and where possible their compliance officer or line manager, which confirms that they can accept the gift or hospitality as it is in line with their own organisation's policy and the law of their country. You should contact the Ethics and Compliance team to discuss the options for getting this confirmation.

There are a number of other scenarios where there are rules in place when engaging with public officials:

1. Employment/internships - Employment decisions, including paid or unpaid internships and secondments, must be based on merit and not made to improperly influence public officials. Accordingly, if a known family member or designee of a

public official is seeking employment at BT, including a secondment or internship, you must obtain pre-approval before proceeding with the recruitment or employment process from the Director of Ethics and Compliance (or their delegate);

2. Charitable Contributions and Donations - Requests from public officials for donations to specific charities or non-profit organisations may be considered bribes if the donation is made to improperly influence any act or decision of that official. Any requests for such charitable contributions or donations must have prior approval from the Director of Ethics and Compliance (or Ethics and Compliance ;
3. Conference and Event Sponsorships and any associated payments may be considered bribes if made to improperly influence any act or decision of a public official. Requests by public officials for BT to sponsor conferences or other events must have prior approval from the Director of Ethics and Compliance (or their Ethics and Compliance);
4. Family members - Providing business courtesies to the family members of a public official is prohibited.

3.4 Additional rules for US Officials

There are strict rules around activities with US officials. We have to make sure we're in line with the Lobbying Disclosure Act. We have to file two separate types of reports on expenditure related to US government officials. One of these reports, which is filed every six months, specifically captures political contributions. This includes donations to Political Action Committees, donations to charities founded by, controlled by or related to US government officials as well as certain gifts, hospitality and sponsored travel.

The definition in US regulations is wide, particularly in relation to donations. In addition to the list above, it also includes things like attending a charity dinner where a US public official was in attendance and received an award in recognition of their support for the charitable cause. Even though BT had not invited the public official, the cost of the BT person attending the event would be classified as a political donation.

The penalties for non-compliance with the US rules for public officials are severe and could be very damaging to our reputation. It's really important that these events are properly recorded. Where these events are not registered centrally as gifts and hospitality or charitable donations, or where it has been registered but the attendance of the public official is not known beforehand, you must notify the Vice President US Government Affairs of the event as soon as possible.

If you need further advice, please ask contact the Ethics and Compliance team or the Vice President US Government Affairs.

3.5 Lobbying

Lobbying describes engagement with policy-makers and other external stakeholders with the intent to represent BT's perspective in the policy-making process.

BT will engage with policy-makers on subjects of legitimate concern to its business, customers and end users and the communities in which it operates. BT will also engage in lobbying activity to provide policy-makers with data and insights to enable informed decision-making. Active contribution to policy-making is an integral part of the democratic process and a legitimate activity as it enables the representation of different societal interests.

BT people engaged in lobbying activity must comply with all requirements of applicable laws and regulations relating to that activity and must act with honesty, integrity and transparency.

Please contact the Public Affairs team before you engage in any lobbying activity.

4 BT's position on Political Donations

BT does not make donations whether in cash, kind, or by any other means, to help with the campaign activities or day-to-day activities of any political party, candidate or of any organisation specifically allied to a political party. We recognise that this may be perceived as an attempt to gain an improper business advantage.

BT does not make donations whether in cash, kind, or by any other means to help with the campaign activities or day-to-day activities of any political party, candidate or of any organisation specifically allied to a political party. Neither will such donations be made to any individual member of a legislature, at local government, regional, national or supranational level or to their staff. We recognise this may be perceived as an attempt to gain an improper business advantage.

A fuller statement of BT's position on political donations can be found here.

4.1 What are political donations?

For the purposes of anti-bribery and corruption law, it is irrelevant whether a person is considered a public official by the government at issue.

1. Political donations are donations made to:
   a) Any registered political party;
   b) Any political party which carries on activities for the purposes of or in connection with the participation of the party in any election to public office;
   c) Any political organisation which carries on activities that are reasonably regarded as intended to:
      I. Affect public support for a political party or independent candidate; or
      II. Influence voters in relation to any national or regional referendum held under the law of the United Kingdom or any other country.

However, the definition of political donations in the UK Companies Act 2006 is wide, covering activities such as making MPs aware of key industry issues, gifts (of money or other property), sponsorship, subscription or membership fees, money spent paying expenses of any political party, loans other than on commercial terms and the provision of any property, services or facilities other than on commercial terms.

All such expenditure must be authorised and operated by the UK and Global Public Affairs Teams.

The definition of political expenditure is wide too. Political expenditure is defined as expenditure incurred on the preparation and publication of advertising or other promotional material which, at the time of publication, is reasonably regarded as intended to affect public support for a political party, other political organisation or independent election candidate. Shareholder approval for expenditure of this kind is sought at the annual general meeting each year. A specific record of expenditure of this kind must be kept, as the total is disclosed in BT's Annual Report. Therefore, you need to report and get authorisation from your regional Public Affairs team before committing to any political expenditure.

Click here to see if there are any additional in-country specific requirements relating to public officials. For further guidance, please ask the Ethics and Compliance team.

5 Responsibilities

Bribery is subject to laws and controls worldwide and there are serious penalties for anyone, or any company, breaking these laws including unlimited fines and imprisonment.

Anyone involved in facilitation payments or “kickbacks” may be subject to disciplinary action, including dismissal and terminating our relationship with individuals and organisations working on our behalf. Any payment may also lead to criminal prosecutions for both the individuals and companies that pay them.

BT’s position on Facilitation Payments, Blackmail and Extortion and Public Officials and Political Donations are mandatory. This Guidance document is to help you make informed decisions. We expect everyone acting on BT’s behalf to read, understand and use this Guidance.

6 Other related topics

There are a number of topics which are related to the risks of bribery and corruption. They form part of our programme to prevent, detect and respond to these risks. Further related documents are available on these topics:

1. Anti-Bribery and Corruption Standard
2. Gifts and Hospitality Standard and Guidance
3. Conflicts of Interest Standard and Guidance

7 Speak Up about your concerns

If you are worried you've spotted something unethical, or something that makes you feel uneasy at work, do the right thing and contact Speak Up.

Speak Up is a safe and confidential way for you to help protect yourself, BT and live our values. Don't rely on someone else, get in touch yourself. We can't act on your concerns if we don't know about them. For further information on Speak Up, please see the Speak Up intranet pages.

If you are a BT employee and have any questions about this Standard, speak to the Ethics and Compliance Team.

Version Control

Version	Approval Date	Reason for Change
1.0	15 March 2022	Updated to new Standards template
2.0	October 2022	Updated to new Standards template