Bupa

Bupa Policies

Suppliers Handbook

Purpose of this handbook

This handbook serves Bupa's third party suppliers as a reference guide for all relevant Bupa Policies.

The aim of this handbook is to ensure suppliers have a high level understanding of Bupa's relevant policies and support Bupa in meeting our business objectives and ensuring we safeguard our customers and people.

Specific details in relation to the scope of services provided, terms and conditions and contractual obligations are detailed in the signed contract between Bupa and you.

Why is this important

Suppliers constitute an important part of Bupa's environment. We rely on a range of suppliers for the provision of products and services, as such we have an obligation to ensure we manage all risks within our supply chain. In partnership with our suppliers we create positive impacts for:

Our customers: by protecting our customers from any detriment or harm and ensuring Bupa continues to be a strong company, able to deliver on our promises.

Our people: by protecting our people from harm and giving everyone the right systems, knowledge, and tools to identify, mitigate, and respond to risks in the right way.

Our regulators: by providing assurance that we meet and, where possible, exceed regulatory expectations.

Bupa: by equipping Bupa to achieve its objectives, reaching desired financial outcomes, protecting our reputation and continuing to grow our business in a sustainable way.

Controls: to deliver policy requirements must be built into processes, procedures, work instructions and training material.

In addition to this Supplier Handbook, please refer to Bupa's Responsible Supply Chain Statement which sets the minimum standards of business conduct that Bupa expects from our direct suppliers and that need to be applied in turn, through the supply chain.

Bupa Policies

We expect our suppliers to have suitable controls in place, such as processes, procedures, work instructions and training, to ensure compliance with the following Bupa Policies' Principles.

Brand and Reputation Policy Key Principles
1. Reputation and Brand
1.1. We all have the potential to impact Bupa's reputation and brand through communications, behaviour, actions or inaction.
1.2. We consider reputation and brand through the eyes of our stakeholders, including our customers, our people, our business partners, our regulators, policymakers, the media and wider society.
1.3. We see that reputation and brand is interconnected between geographies and across business lines. We are proactive in identifying and managing risks and interdependencies.
1.4. We assess all business risks for reputational and brand impact and take a proactive approach to identifying, monitoring and mitigating reputation risk.
1.5. We regularly refresh our understanding of reputation management and our preparedness, through training and exercises.
1.6. We measure reputation in our markets and use insights and data to improve our communications and business activity.
1.7. We understand that inaction can be as damaging to our brand and reputation as taking the wrong action.

2. **Communications**

   2.1. We engage transparently with the media, and on social media, to promote and protect our reputation and brand and to communicate with audiences.

   2.2. We consult Corporate Affairs in advance for communications plans and content, including social media.

   2.3. We encourage our people to use social media responsibly in line with local policies and our values.

   2.4. We take a joined-up approach, knowing our audiences often see us as 'one Bupa'. For example, we understand that internal communications can become external, and we develop messaging accordingly.

   2.5. We proactively manage external and internal information about Bupa to ensure it is relevant and accurate. For example, Bupa website content.

   2.6. We engage, inform and empower our people through internal communications and equip them with relevant tools and advice.

   2.7. We communicate with our customers directly, honestly and authentically, tailoring messages and providing two-way feedback mechanisms.

   2.8. We prioritise our customers' communication needs and view our programmes and strategies through their eyes.

   2.9. Bupa is politically neutral. We work constructively with governments and parties across the political spectrum. We engage proactively and transparently, acting in accordance with the Bupa Code and local laws.

   2.10. All external and internal communications about financial performance, strategic issues, significant acquisitions and divestments are managed in consultation with the Group Corporate Affairs and Finance teams ahead of any communication. This includes preparing for any leaks and approval timelines for the Bupa Executive Disclosure Committee (BEDC).

3. **Issues and Crisis Communications**

   3.1. We escalate potential and live issues which could impact Bupa's reputation

   3.2. We ensure we are prepared to communicate internally and externally during an issue or crisis.

   Our Brand

   4.1. Proper use and protection of our brand is essential to our reputation. We make sure all elements of brand management are robust and implemented consistently across all touch points.

   4.2. We protect our brand ownership and rights by preventing any misuse of our trademarks and domain names.

Conflict of Interest Policy Key Principles

1. **Legal and Regulatory requirements**

   1.1. In many instances, Bupa's regulators around the globe have issued rules and guidance on conflicts of interest. We will comply with these rules and guidance as applicable. We understand that inaction can be as damaging to our brand and reputation as taking the wrong action

2. **Conflicts of Interest Framework**

   2.1. Bupa takes all reasonable steps to operate effective organisational arrangements to prevent actual or potential conflicts of interest from causing a material risk of detriment to our customers or damage to our reputation.

   2.2. We implement procedures and measures to identify and manage conflicts of interest.

3. **Record-keeping**

   3.1. We maintain records of all conflicts of interest identified within our business.

4. **Reporting**

4.1.	We ensure that appropriate reporting is produced on conflicts of interest

Corporate Responsibility and Sustainability Policy Key Principles

1. CRS Strategy

    1.1. Bupa is committed to being a responsible and sustainable business. Our purpose, helping people live longer, healthier, happier lives, is at the core of our approach to corporate responsibility and sustainability

Customer Outcomes Policy Key Principles

1. People and culture

    1.1. Bupa's Board and senior management create and maintain a culture and environment in which Bupa's behaviours and actions ensure the delivery of fair outcomes for customers.

2. Products and services

    2.1. Bupa's new and existing products and services meet the needs of their target market.

    2.2. Bupa only sells products and services to customers for whom they are suitable.

    2.3. Where external suppliers provide services to Bupa customers on behalf of Bupa, Bupa ensures that the supplier delivers fair customer outcomes that are within Bupa's conduct risk appetite and the requirements of this policy.

3. Sales

    3.1. Bupa takes all reasonable steps to ensure that sales of our products and services are in the best interests of customers.

4. Communications

    4.1. Bupa's customer communications are designed to be clear, fair and not misleading and remain so throughout their lifetime.

5. Service

    5.1. Bupa's customer service processes are designed in response to the needs of customers.

6. Complaints

    6.1. Bupa uses insights from complaints to improve customer outcomes.

7. Governance

    7.1. Bupa embeds awareness of fair customer outcomes in the organisation by setting the tone from the top, raising awareness, and training our people.

Financial Crime Risk Policy Key Principles

1. We set the tone from the top

    1.1. We set the tone from the top by demonstrating top level leadership commitment to establish and maintain an effective Financial Crime compliance culture.

2. We establish a governance framework that sets clear accountabilities for managing Financial Crime Risk

    2.1. There is effective governance oversight, we assign appropriately skilled resources to assist with the management of Financial Crime Risk and train our people to help them identify and assist with its management.

3. We understand and properly assess Financial Crime Risk

3.1. We undertake regular assessments of Financial Crime Risk to support a risk-based approach to our control framework.

4. **We implement controls to manage Financial Crime Risk effectively**

    4.1. We implement, maintain and as required, update an appropriate control framework (informed by our risk assessments) to manage Financial Crime Risk effectively

5. **We monitor and report on Financial Crime Risk and escalate incidents**

    5.1. We develop accurate management information and record and escalate incidents.

Information Security Policy Key Principles

1. **We govern, and manage risk to Information Security effectively**

    1.1. The management of information security must follow a defined governance model, including management bodies which are comprised of accountable members with appropriate authority.

    1.2. The governance model must also ensure that we continually monitor and review our compliance and effectiveness of our information safeguards.

2. **We manage and protect information using appropriate business processes techniques and technology**

    2.1. Information security is implemented and applied using business processes, techniques and technologies which are appropriate to maintain confidentiality, integrity and availability These must be fit for purpose and evolve through continuous improvement with technological advances and changes to business processes.

    2.2. This includes raising awareness of, and educating all Bupa people on, information security and acceptable usage to protect the confidentiality, integrity and availability of Bupa information.

3. **We monitor emerging and existing threats to ensure defences remain effective**

    3.1. Information Security frameworks must continuously monitor and adapt to the risks from new and emerging threats. This must ensure our information security defences and controls remain effective and adapt where necessary to the changing threats to our information and systems.

4. **We respond to Information Security Incidents in a timely and robust manner**

    4.1. When information security incidents occur, the response must identify, validate, contain and minimise root cause weaknesses to allow for timely recovery and remediation to minimise the impact on business processes.

Modern Slavery Act

1.1. The MSA 2015 defines slavery or forced labour as holding 'another person in slavery or servitude and the circumstances are such that the person knows or ought to know that the other person is held in slavery or servitude'. Slavery is a violation of a person's human rights. It can take the form of human trafficking, forced labour, bonded labour, forced or servile marriage, descent-based slavery and domestic slavery.

1.2. A person is considered to be in modern slavery if they are:

- Forced to work through mental or physical threat
- Owned or controlled by an "employer", usually through mental or physical abuse
- Dehumanised, treated as a commodity or sold or bought as "property"
- Physically constrained or has restrictions placed on their freedom of movement

1.3. We have provided below a list of useful links to resources, guides and information. We strongly encourage our suppliers to refer to these in order to ensure they are fully informed about the MSA 2015.

- UK Government:

  https://www.gov.uk/government/publications/modern-slavery-industry-factsheets
  https://www.gov.uk/government/publications/transparency-in-supply-chains-a-practical-guide

- Chartered Institute of Purchasing and Supply (CIPS):

  http://www.cips.org/en/Supply-Management/Analysis/2016/February/Think-your-supply-chain-is-free-of-slavery-Think-again/

Operational Resilience Policy Key Principles

1. **Governance**

    1.1. Bupa is committed to effective management and governance of operational resilience, with executive and Board accountability and oversight.

    1.2. Bupa's operational resilience capability is proportionate with its businesses' risk profile. It is designed to protect customers and our people, support Bupa's reputation and long-term business sustainability, and meet regulatory obligations, where they exist.

2. **Awareness**

    2.1. Bupa embeds operational resilience in the organisation by setting the tone from the top, raising awareness, and training our people.

3. **Analysis**

    3.1. Bupa determines critical business services that must be protected as a priority, from the perspective of customers, and sets impact tolerances, within which those services must be restored.

    3.2. Bupa understands the resilience capability of components that underpin critical business services.

    3.3. Bupa identifies threats, trends and change that could result in operational disruption.

    3.4. Bupa builds operational resilience by design.

4. **Implementation**

    4.1. Bupa establishes controls to reduce the risk of operational disruption and develops capability to respond and recover when disruption happens.

    4.2. Bupa prepares for a range of scenario and impacts, in line with the operational risk appetite and operational resilience risks.

5. **Validation**

    5.1. Bupa assesses the effectiveness of its operational resilience capability and improves continuously by performing regular tests and reviews, taking an integrated approach, and by learning from incidents and near misses, in line with the Enterprise Incident Management Policy.

Privacy Policy Key Principles

1. **We use data fairly and lawfully and we're transparent about how we use it**

    1.1. When we process data about individuals, we ensure that they are appropriately informed about what we're collecting, why we are collecting it, how we will use it and who we are going to share it with.

    1.2. Our processing is always based on lawful grounds and when we've told individuals the purposes of our processing we won't use it for an incompatible purpose, unless the law allows us to.

2. **We keep data accurate and up to date**

2.1. We regularly check the accuracy of data and ensure it's up to date and provide the opportunity for individuals to check and update it themselves

3. **We use data that is adequate and relevant**

   3.1. We ensure data is adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

4. **We don't keep data for longer than we need to**

   4.1. When we no longer need data and there is no legal reason to retain it, we anonymise it or securely dispose of it.

5. **We respect individuals' rights**

   5.1. We respect the legal rights of individuals, and we comply with our obligations that arise from their exercise of those rights

6. **We process data securely**

   6.1. We protect data with appropriate technical and organisational security measures

7. **We design with privacy built in**

   7.1. We assess the privacy impact of our processing data on individuals and build in privacy right from the start (and throughout the data lifecycle).

8. **We process data ethically**

   8.1. We ensure the use of tools and technologies that involve monitoring, tracking, profiling or which could intrude in any way on an individual's privacy, is ethical.

Risk Management Policy Key Principles

1. **Governance**

   1.1. The Board has overall responsibility for the oversight of risk across Bupa and for ensuring risk management activities are embedded across Bupa.

2. **Culture and Responsibilities**

   2.1. The Chief Executive Committee members set a strong ''Tone from the Top'' with regards to risk management and have accountabilities for facilitating and supporting a strong culture for risk management across Bupa.2.2Risk management outputs are used to inform Bupa's strategy, risk appetite, business decision making and capital planning.

3. **Risk Appetite**

   3.1. The Board Risk Appetite Statements, as defined by the Bupa Board, apply across Bupa, and set out the type and amount of risk that the Board is willing to take.

4. **Risk Management Framework**

   4.1. The Risk Management Framework is implemented across Bupa to ensure a consistent approach to risk management.

   4.2. Enterprise-wide policies are maintained and define the key principles and requirements for how specific risks are managed as well as the risk thresholds, key indicators and minimum controls to support the management and monitoring of the risks.

5. **Risk Management in Change**

   5.1. Bupa implements strategies to manage the risk in effecting change, controlling change and helping people to adapt to change.

6. **Process management**

   6.1. Bupa avoids failures or errors in processing or process management that could result in losses and/or adverse impacts on stakeholders.

Speak Up Policy Key Principles

1. Promoting Speak Up

    1.1. We want to know about any breach or potential breach of our policies and standards, or any wrongdoing or risk of harm, to our people, customers, the public, the environment or Bupa that may be occurring despite our rigorous compliance procedures. We take appropriate steps to ensure that our people feel able to report genuine concerns to us about such matters without fear of negative consequences and that they also see it as their duty to do so. The role of the Speak Up Policy is to provide a means for our people to report such issues and concerns in circumstances where they do not feel able to report the issues and concerns to their line manager or they have done so but do not believe that the issues have been dealt with appropriately.

2. Reporting Speak Up concerns

    2.1. Our people are informed of how to report concerns to us under this Policy or to a regulator in appropriate circumstances and are able to report them confidentially and anonymously if they wish, save that we may, in certain circumstances, be required to disclose information and identities of individuals by law, for the purpose of legal proceedings or government investigations, in order to carry out an investigation, to implement any recommendations following an investigation, to take appropriate action to protect individuals from harm, for audit and compliance purposes or in accordance with the rules of relevant professional bodies.

3. Responding to Speak Up concerns

    3.1. We:
- Take seriously all concerns that are reported to us and investigate them appropriately using existing processes and procedures as appropriate;
- provide appropriate progress updates and feedback to the individual who has raised the concern;
- track the progress of each case and take action when required to ensure that issues are appropriately addressed and any lessons learnt;
- report actual or suspected breaches of law to the relevant law enforcement agencies, where appropriate;
- carry out a review in cases where the individual raising the concern is dissatisfied with the way in which it has been handled; and
- do not allow decisions concerning speaking up within Bupa to be influenced by race, sex, pregnancy or potential pregnancy, maternity, colour, sexual orientation, gender identity/expression/history, transgender or transsexual status, political belie for activity, religion, marital status, caring responsibilities, parental status, breastfeeding, irrelevant criminal or medical record, national or ethnic origin, disability, age, citizenship or membership of a representative body except where required or justified by any applicable laws.

    3.2. If we conclude that an individual has made false allegations maliciously, they may be subject to disciplinary action up to and including summary dismissal. In those circumstances we may also inform the person against whom the allegations have been made.

4. Protection & Support

    4.1. We take appropriate steps to ensure that our people who report genuine concerns are protected from negative consequences. We will not tolerate harassment or retaliation of any kind against anyone who seeks advice or raises a genuine concern covered by this Policy. Anyone who subjects a reporter to such treatment will face serious consequences which may include disciplinary action or dismissal. We also act appropriately having regard to the interests of those about whom Speak Up reports are made.

5. Resourcing and training

    5.1. We dedicate the required level of skilled and other resources necessary to ensure that we fully comply with this Policy. In particular we ensure that all our people who play a formal role in the operation of this Policy are appropriately skilled and trained and are clear about their roles and responsibilities.

6. Legal and regulatory compliance

6.1. We comply with applicable laws and regulations relating to whistle blowing.

7. Record Keeping

7.1. Appropriate records of concerns raised under this Policy and of investigations including their conclusions are retained securely and confidentially

8. Controls, implementation and monitoring

8.1. We take appropriate steps to ensure that this Policy is complied with and that it operates effectively and consistently across Bupa.

Suppliers Policy Key Principles

1. Knowing our Suppliers

1.1. We have a record of our Suppliers, where the supply base is categorised and segmented by spend, type and the impact on customers and the business in accordance with local requirements. We have identified our or Important Outsourcers.

2. Selecting our Suppliers

2.1. We select our Suppliers diligently, ensuring they are a good fit with Bupa and our business needs, ensuring they have adequate governance and operational controls in place to meet the needs of our customers.

3. Contracting with our Suppliers

3.1. We ensure appropriate contracts are in place with our Suppliers covering the relevant product or service requirements and applicable customer, legal and regulatory requirements.

4. Managing our Suppliers

4.1. Based on the segmentation of Suppliers, we continuously monitor and manage the performance of our Suppliers to ensure they continue to meet our customer and business needs and are meeting standards expected of a supplier and under the relevant contractual arrangements.

Outsourcing Policy Key Principles

1. Systems of Governance

1.1. Where FCA and/ or PRA regulated, Bupa must have in place an effective system of governance that provides for the sound management of our outsourcing arrangements.

2. Record Keeping

2.1. Where FCA and/ or PRA regulated, Bupa must arrange for orderly records to be kept of its outsourcing arrangements.

3. Materiality Assessment

3.1. Where FCA and/ or PRA regulated, Bupa must assess the materiality of their outsourcing and third-party arrangements.

4. Regulatory Notification of Material Outsourcing

4.1. Where FCA and/ or PRA regulated, Bupa will inform the PRA and/or the FCA in a timely manner about planned material outsourcing arrangements or significant changes in a material outsourcing arrangement.

5. Risk Assessment

5.1. Where FCA and/ or PRA regulated, Bupa will assess the potential impact of outsourcing arrangements on their operational risks, take into account the assessment results when deciding if the function should be outsourced to an outsourced supplier; and take appropriate steps to avoid undue additional operational risks before either entering into or during an outsourcing arrangement.

6. **Due Diligence**

   6.1. Where FCA and/ or PRA regulated, Bupa will conduct appropriate due diligence on a potential outsourcing supplier before entering into an outsourcing arrangement.

7. **Contractual Arrangements**

   7.1. The rights and obligations of Bupa and the outsourcing supplier should be clearly allocated and set out in a written agreement.

8. **Business Continuity and Exit Plans**

   8.1. Where FCA and/ or PRA regulated, Bupa must have appropriate business continuity and exit plans designed to anticipate, withstand, respond to and recover from severe but plausible operational disruptions that impact upon the delivery of outsourced functions.

9. **Managing Outsourced Arrangements**

   9.1. Where FCA and/ or PRA regulated, Bupa will effectively supervise outsourced arrangements to ensure they continue to provide services that meet the needs of our customers and our business and comply with contractual arrangements, applicable laws, regulatory requirements and any other relevant Bupa policies.

Technology Risk Policy Key Principles

1. **Technology Operations**

   1.1. Adequate and rigorous controls are in place to mitigate against the risks of non-availability of technology Systems. This is to ensure that the technology risk around operation of technology systems within the BUPA Group is understood, monitored, and mitigated appropriately. Also, to give a level of assurance that day to day technology operations remains compliant with the requirement of the Group Risk Management Framework (RMF).

2. **Technology Change**

   2.1. Adequate and rigorous controls are in place to mitigate against the risks of inadequate design, testing or implementation of new or changed technology Systems.

   2.2. This is to ensure that technology risk is assessed, understood, monitored, and mitigated appropriately around changes to technology systems and infrastructure - either new or existing, within the BUPA Group.