1. INTRODUCTION

- This privacy notice is issued on behalf of British-American Tobacco (Holdings) Limited ("BAT"), which is a data controller of your personal data and is a member of the BAT group of companies ("BAT Group").

- The principles governing Speaking Up about suspected wrongdoing at work are addressed in the BAT Group's Speak Up Policy which forms part of our Standards of Business Conduct ("SoBC"). The Speak Up Policy sets out information on how reports made via one of the Speak Up channels are managed. It can be found by accessing the SoBC at www.bat.com:
  https://www.bat.com/group/sites/UK__9D9KCY.nsf/vwPagesWebLive/DO9EAMHQ

- BAT take any allegations of actual or suspected wrongdoing seriously and we encourage you to Speak Up should you have any such concerns. To do so, you can contact one of our confidential, independently managed external Speak Up channels (available at www.bat.com/speakup which includes a web-based reporting tool and a list of global Speak Up hotline numbers), collectively called the "Speak Up Hotline".

- When you raise a concern using the Speak Up Hotline, BAT will review your concern promptly and in accordance with its internal procedures for the management of such concerns. Any allegation of a breach of the SoBC will be investigated fairly and objectively and maintaining appropriate confidentiality. BAT will provide you with feedback provided we are able to contact you.

2. SCOPE OF THIS PRIVACY NOTICE

- This privacy notice applies to all BAT Group company employees as well as any non-employee who raises a concern via BAT's Speak Up Hotline. Use of the Speak Up Hotline is voluntary. If you choose to use it to report an issue, we will need to process your personal data in order to investigate your report and meet our regulatory requirements.

- This privacy notice explains what BAT do with your personal data from the point at which you raise concerns via the Speak Up Hotline. Generally, it describes how your personal data may be processed when you contact the Speak Up Hotline and, in doing so, how we comply with our legal obligations to you.

- When we say "we" or "us" in this document, we mean British-American Tobacco (Holdings) Limited which is the data controller of any of your personal information processed for the Speak Up Hotline.

- Your privacy is important to us, and we are committed to protecting and safeguarding your rights. In this privacy notice, when we refer to compliance with data protection laws we are also referring to the "GDPR", meaning the General Data Protection Regulation, which is a European law governing your rights in relation to your personal data, and how organisations should protect it.

- We may amend this privacy notice from time to time. Please visit this page if you want to stay up to date.

3. WHAT CAN I REPORT VIA THE SPEAK UP HOTLINE?
The Speak Up Hotline allows employees or non-employees to report any concerns they may have about actual or suspected wrongdoing within or connected with the BAT Group. Examples of wrongdoing include:

- criminal acts, including theft, fraud, bribery and corruption
- endangering the health or safety of an individual or damaging the environment
- bullying, harassment (including sexual harassment) and discrimination in the workplace, or other human rights abuses
- accounting malpractice or falsifying documents
- other breaches of the SoBC or other global policies, principles or standards of the BAT Group;
- failing to comply with any legal obligation, by act or omission
- a miscarriage of justice
- concealing any wrongdoing.

4. WHAT PERSONAL DATA MIGHT BE PROCESSED WHEN I USE THE SPEAK UP HOTLINE?

BAT may collect, process and use certain categories and types of personal data about you in connection with reports you make to the Speak Up Hotline, or when investigating a report that has been made to the Speak Up Hotline which concerns or is connected to you. The specific categories of your personal data processed or used in an investigation will depend on the nature of the report and whether you are an employee or non-employee, and are likely to include

- **identification data**, such as your name, employee/Staff ID, business email address, home email address if that is the email address through which you have made the report, business address, business landline;
- **information about your job**, such as your position, business title, employee type, management level, work location, division, department and position level, job history (including position history, title history, effective dates and past pay groups);
- **alleged facts reported**;
- **information collected in connection with the investigation of the reported facts**;
- **information collected in connection with any connected investigation**;
- **information about your salary and benefits**, such as your basic salary, bonus and commission entitlements, raise amounts and percentages, allowances, compensation for on-call duties, and insurance benefits, pension plans, tax code, your bank account details and payment dates, accrued salary information, employee pay group, information relating to your pension;
- **time and systems / buildings access monitoring information**, such as CCTV images, swipe card access, time recording software, internet, email and telephone usage data; and
- **performance and disciplinary information**, such as performance reviews, evaluations and ratings, information about disciplinary allegations, the disciplinary process and any disciplinary warnings, details of grievances and any outcome;

and the following **sensitive categories** of personal data:

- **health and medical data**, such as medical conditions, sickness absence, and reasons for it, for instance if the report made concerns work-related accidents, or other workplace health and safety considerations, or allegations of disability or maternity related discrimination;
- **criminal records data**, if the report concerns alleged past or ongoing criminal conduct, and BAT for instance obtains a criminal records check;
- **race, ethnicity, or sexual orientation data**, for instance if the report concerns workplace harassment, bullying or discrimination on one of these protected grounds,

together "Speak Up Hotline Data".

- No Speak Up Hotline Data will be used for automated decision-making.

5. WHY IS THIS INFORMATION BEING COLLECTED?

- Disclosures via the Speak Up Hotline are voluntary. If you choose to use the Speak Up Hotline to report an issue, we will have to process your Speak Up Hotline Data to review your report and to investigate the issue you've raised. BAT is therefore likely to have a legitimate interest in processing such data for this purpose. However, when considering whether processing your data is within our legitimate interests, we will carry out a balancing exercise between our interests and your rights and freedoms, to ensure it is appropriate for us to go ahead. We will also identify any extra steps we need to take to protect your rights.

- As well as BAT's legitimate interests, BAT may collect and use this Speak Up Hotline Data for other reasons linked to our regulatory obligations and (where relevant) your employment, including:
  - **to comply with applicable laws and employment-related requirements** which involves the processing of identification data, information about your job, performance and disciplinary information; and
  - **to monitor compliance with applicable laws and BAT Group policies and procedures**, including conducting internal investigations, which involves the processing of identification data, information about your job, information about salary and benefits, time and systems/building access monitoring information, and performance and disciplinary information.

6. WHO MIGHT MY INFORMATION BE SHARED WITH?

- The current Speak Up Hotline operator is a company called Convercent (who is a data processor on behalf of BAT). Your personal data will be shared with Convercent. Convercent provides the reporting platform and Speak Up Hotline that you can use to raise issues and is subject to contractual obligations to implement appropriate security measures to safeguard your personal data, and to process the personal data only as instructed by BAT.

- In certain circumstances it may be necessary for BAT to pass your data to third parties in the UK or in other jurisdictions to investigate your concerns. This might include:
  - any of our BAT Group companies (a full list is available from www.bat.com);
  - Tax, audit, or other authorities, when we believe we are legally required to do so, where the relevant authority has asked us to assist (for example, because of a request by a tax authority or in connection with any expected litigation), or in order to help prevent fraud or to protect the rights of BAT; or protect the personal safety of BAT employees, third party agents or members of the public;
  - third party service providers such as external consultants and professional advisers (including law firms, auditors and accountants), technical support functions, and IT consultants carrying out testing and development work on our business technology systems);
o third party outsourced IT providers, including but not limited to email/text messaging providers; Cloud IT service providers, business suite solution providers; data analytics agencies; IT strategic implementation partners; hosting service providers;

o if it is proposed that a BAT Group entity or business is to merge with or be acquired by another business in the future, we may share your personal information with potential purchasers, where this is necessary, or the new owners of the business or company.

• Some countries already provide an adequate level of protection for this data (such as Switzerland). If recipients are located in other countries without these protections, BAT will take all necessary measures to ensure that transfers out of the EEA are adequately protected as required by applicable data protection law.

• If you have any queries in relation to how your data may be processed outside of the UK, employees should contact their local LEX Counsel, or a local Designated Officer or Business Integrity Panel. Non-employees can contact the applicable data protection authority in their jurisdiction.

7. MY DATA RIGHTS

• You have a number of rights in relation to your Speak Up Hotline Data. These include:

  o Right of access including the right to confirm whether your personal data is processed, and if it is, to request access to that personal data;

  o Right to rectification of inaccurate or incomplete personal data concerning you;

  o Right to erasure (right to be forgotten);

  o Right to restriction of processing;

  o Right to data portability;

  o Right to object to processing;

  o Right to withdraw consent to the processing of your data; and

  o Right to file a complaint with the local data protection authority.

• Employees can find more information on their data rights within the BAT Group Employee Privacy Notice. Non-employees can view the BAT Privacy Notice online here.

8. HOW LONG WILL MY DATA BE RETAINED?

• Your Speak Up Hotline Data will be kept as long as necessary to process and investigate the report, or, if applicable, as long as necessary to initiate sanctions or to meet any legal or financial requirement, or as is appropriate for any applicable limitation period. In any case, if judicial or disciplinary proceedings are initiated, the personal data provided will be kept until those proceedings are definitively closed. For further information about applicable retention periods please email us at data_privacy@bat.com.

9. CONTACT

• If you have questions regarding this privacy notice, or would like to exercise any of the rights referred to above, please email contact us at data_privacy@bat.com.