

Employee Handbook

Bamboo Medical Communications Ltd.

Version 1

Date: January 2024

Contents

1.1 Preface	5
1.2 About Bamboo Medical Communications Ltd.	6
1.3 Legal Disclaimer	7
1.4 Terms and Conditions of Employment	7
2 ATTENDANCE/TIME OFF/LEAVES OF ABSENCE	8
2.1 Attendance and Punctuality	8
2.2 Reporting Absences	8
2.3 Annual Leave	8
2.4 UK Bank Holidays	9
2.5 Bereavement Leave	9
2.6 Parental Leave	9
2.7 Extraordinary Paid Leave	11
2.8 Hours of Work	11
3 COMPENSATION	11
3.1 Payment of Wages	11
3.2 Income Tax	11
3.3 Expense Reporting Policy and Procedure	12
4 POLICIES	12
4.1 Verification of Employment and Paid Survey's	12
4.2 Open Door	12
4.3 Equal Opportunity	12
4.4 Anti-Harassment	13
4.5 Employment of Relatives, Nepotism, and No-Fraternizing Policy	13
4.6 Dress Code	14
4.7 Inclement Weather and Emergency Closing	14
4.8 Background and Credit Screening	14
4.9 Non-Disclosure/Confidentiality	14
4.10 Contact with the Media	15

4.11 Continuing Education	15
4.12 Contracts	15
4.13 Personnel Records	15
4.14 Sick Pay Provision	15
4.15 Fit for Duty	16
4.16 Return of Property	16
4.17 Solicitation	16
4.18 Outside Employment	16
4.19 Employee Conduct and Work Rules	17
4.20 Business Ethics and Conduct	17
4.21 Disciplinary Procedure	18
4.22 Performance Evaluation & Management, Career Development	19
4.23 Conflict of Interest	19
4.24 Acceptance of Gifts	20
4.25 Work Product Ownership	20
4.26 Remote Working Policy/Flexible Working Policy	20
4.27 Company Equipment	21
4.28 Environmental Policy	21
4.29 Whistleblower Policy	22
4.30 Data Security and Privacy Policy	22
5 WORKPLACE SAFETY	26
5.1 Controlled Substances	26
5.2 Drug Testing	27
5.3 Smoking	27
5.4 Workplace Violence	27
5.5 Employers Liability Insurance	27
6 ELECTRONIC DEVICES	28
6.1 General	28
6.2 Telephones and Personal Electronics	28
6.3 Company Mobile Policy	29

6.4 Computer and Internet	30
6.5 Software Downloads	30
6.6 Email	31
6.7 Social Media Policy	32
6.8 BYOD (Bring Your Own Device) Policy	34
BAMBOO GDPR COMPLIANCE POLICY	36
1 Purpose	36
2 Scope	36
3 Policy Statement	36
3.1. Governance	36
3.2. Data Protection Principles	38
3.3. Data collection	38
3.4. Data Use	39
4 ROLES AND RESPONSIBILITIES	44
5 Review	44
6 Records Management	44
7 Terms And Definitions	44
8 Related Legislation And Documents	45
Bamboo Data Subject Access Request Policy And Procedure	46
1. Purpose	46
2. Scope	46
3. Policy Statement	46
4. Procedure	46
5. Responsibilities	48
6. Terms And Definitions	48
7. Related Legislation and Documents	49
7 ACKNOWLEDGEMENTS	50
7.1 Receipt and Acknowledgement of Handbook	50

1.1 PREFACE

This Employee Handbook ("Handbook") applies to Employees of Bamboo Medical Communications Ltd. ("Bamboo") an Aptitude Health Company and supersedes and replaces all earlier versions and/or editions. This Handbook has been written to serve as the guide for the relationship between you ("Employee") and your employer. It is also designed to provide basic information on certain policies and procedures in place at the Company. There are several things to keep in mind about this Handbook. The policies in this Handbook are intended as guidelines only and are subject to change or elimination at the sole discretion of the Company, depending on the policy. This Handbook is not intended to be comprehensive or to address all the possible applications of, or exceptions to, the general policies and procedures described herein. For that reason, if you have any questions concerning eligibility for a particular benefit, or the applicability of a policy or practice to you, you should address your specific questions to the Human Resources ("HR") Department. You should become familiar with the contents of this edition of the Handbook. This document is designed to be an informational resource about many of the benefits, policies, and work practices that affect employment. As an informational resource, this Handbook is not all inclusive, but rather is a quick reference guide to assist you, the Employee.

Nothing contained in this Handbook creates an employment contract, either expressed or implied.

The Company retains the right to interpret, modify or eliminate benefits, policies, or procedures as circumstances warrant. The Company will communicate such changes to Employees. This Handbook and the information contained herein should be treated as confidential. No portion of this Handbook should be disclosed to others, except Employees of the Company and others affiliated with the Company whose knowledge of the information is required in the normal course of business.

1.2 ABOUT BAMBOO MEDICAL COMMUNICATIONS LTD.

Dear Employee,

Welcome to Bamboo, an Aptitude Health Company. We are happy that you are part of our global, highly skilled staff, who strive to improve healthcare and patient lives in a fast-paced environment.

At Bamboo Medical Communications we offer tailored solutions for our clients' marketing needs. Our aim is for activities that we undertake to be fully integrated where appropriate and consider how the project fits in to the strategic plans for the product.

We focus on face-to-face communications (meetings and events, sales force effectiveness) and digital communications (web-based activities, video/audio content for web or off-line solutions) and many other projects suitable for the pharmaceutical industry.

We want to assist our clients in moving closer to their marketing goals and ensure that all communications to customers are part of a linked strategic journey.

We celebrate diversity and are committed to fostering an inclusive environment. We believe that diverse perspectives, backgrounds, and experiences contribute to our innovation and success. We embrace individuals of all races, ethnicities, genders, sexual orientations, abilities, and backgrounds, recognizing that our collective differences make us stronger. We strive to create a workplace that values and respects each person's uniqueness, and we are dedicated to promoting equality and equity across all aspects of our organization.

We wish you personal and professional success within Bamboo.

1.3 LEGAL DISCLAIMER

This Handbook is designed to provide essential information on certain policies and procedures at Bamboo. The policies contained in this handbook are subject to change at the sole discretion of Bamboo, or authorized parties.

This Handbook should not be construed as, and does not constitute, a contract, express or implied, or a guarantee of employment for any specific duration or condition of employment.

Country local laws or individual circumstances may require the addition, elimination, or amendment of individual policies contained in this Handbook.

1.4 TERMS AND CONDITIONS OF EMPLOYMENT

As an employee of Bamboo, you will receive a Contract of Employment outlining specific terms and conditions of service as they relate to your job. This includes details of:

- The names of the employer and the employee;
- The date when the employment (and the period of continuous employment) began;
- Remuneration and the intervals at which it is to be paid;
- Hours of work;
- Holiday entitlement;
- Entitlement to sick leave, including any entitlement to sick pay;
- The entitlement of employer and employee to notice of termination;
- Job title (or a brief job description);
- Where it is not permanent, the period for which the employment is expected to continue or, if it is for a fixed term, the date when it is to end.
- Either the place of work or, if required to work in more than one location, an indication of this and of the employer's address; and
- Details of the existence of any relevant collective agreements which directly affect the terms and conditions of your employment.

Probation Periods:

All new staff are subject to a probationary period as indicated in your Contract of Employment. A formal review will take place after 3 months with your direct manager. Your appointment will be confirmed on satisfactory completion of the probationary period. During this probationary period, you will be given appropriate support and development opportunity to help you reach the required standards. Extension of the probationary period may be granted to enable the required standards to be achieved, but failure to do so could result in termination of your employment.

Notice Periods:

Unless your employment is terminated by agreement, or specified otherwise in your principal statement of terms and conditions, you or the Company are required to give a period of notice in writing as follows:

The statutory redundancy notice periods are:

- At least one week's notice if employed between one month and 2 years

- One week's notice for each year if employed between 2 and 12 years
- 12 weeks' notice if employed for 12 years or more as agreed to in your contract of employment
- As agreed to in your contract of employment

These periods of notice will apply if you are dismissed on grounds of inefficiency or if your dismissal is the result of disciplinary proceedings in circumstances where summary dismissal is not justified. Your employment may be terminated without notice where dismissal follows disciplinary proceedings.

2 ATTENDANCE/TIME OFF/LEAVES OF ABSENCE

2.1 ATTENDANCE AND PUNCTUALITY

To maintain a safe and productive work environment, the Company expects you to be reliable and punctual in reporting for scheduled work. Absenteeism and tardiness place a burden on other Employees and the business operations of the Company. Each Employee's work is valuable and necessary for the successful operation of the Company. When an Employee is absent or tardy, it disrupts operations, requires reassignment of job responsibilities, may curtail production, and imposes additional work responsibilities onto other Employees. Our objective is not to penalize those Employees who have an occasion to miss because of an emergency, but to prevent excessive tardiness and absenteeism.

Excessive and unexplained tardiness and poor attendance could lead to disciplinary action.

In instances when Employees cannot avoid being late to work or are unable to work as scheduled, they should notify their manager by telephone as soon as possible in advance of the anticipated tardiness or absence. Absent mitigating circumstances, failure of an Employee to contact the manager or another management representative within one (1) hour of the scheduled start of shift will be considered a "no call/no show" that could result in disciplinary action.

2.2 REPORTING ABSENCES

When unable to report to work because of personal illness or any other reason, you must contact your manager immediately and directly by phone to report the nature of the problem and when you expect to return. In cases of prolonged absence, in addition to immediate reporting, it is suggested that you keep your manager updated on your expected return-to-work date

Sickness Payments:

You will receive statutory sick pay during any absence for sickness or injury, subject to the usual waiting days, certification, and other rules. For more details, please see the Handbook Section on Policies.

Employees can take time off work if they're ill. You will need to give your manager proof of being ill if you are ill for more than 7 days. Upon your return we may require a statement of Fitness for Work from your doctor. Further medical certificates are required for the remainder of the period of your absence.

2.3 ANNUAL LEAVE

Employees of the company whether part-time or full-time are entitled to a minimum 25 days of paid annual leave per year pro-rata.

Holidays must be agreed with your manager in advance of taking the time. The Company will where possible try to accommodate individual preferences for holiday dates, but the needs of the business may have to take

precedence, particularly where short or inadequate notice is given. The Company is not responsible for any losses because of holidays being booked prior to authorisation.

- The holiday year runs from 1st January to 31st December.
- Leave for employees joining after the start of the leave year accrues at the rate of one twelfth of the annual entitlement for each complete calendar month of service.
- Leave for employees who terminate their employment during the leave year is calculated on the same basis. If, however, the annual leave entitlement has been exceeded, a deduction calculated on the same basis will be deducted from the final salary payment.
- Holiday pay in lieu of accrued leave will be paid only on termination of employment.

All employees are required to take compulsory annual leave whilst the office is closed between Christmas and New Year.

2.4 UK BANK HOLIDAYS

The following bank holidays are considered paid leave for all active employees:

- New Year's Day
- Good Friday
- Easter Monday
- May Day
- Late May Bank Holiday
- August Bank Holiday
- Christmas Day
- Boxing Day

*** The company closing between Christmas and New Year's is at the discretion of the group CEO.

2.5 BEREAVEMENT LEAVE

In the unfortunate event of a death in the immediate family, a leave of absence of up to 10 days with pay will be granted. These 10 days are to be taken consecutively within a reasonable time of the day of the death or day of the funeral and may not be split or postponed without prior discussion or authorisation.

Immediate family, for purposes of this section, is defined as:

- Spouse
- Child
- Stepchild
- Parents (including in-laws), stepparents.

The Company also provides 4 days of bereavement leave for siblings, step siblings, grandparents, and grandchildren. All other family members such as aunts, uncles, nieces, nephews, or cousins are allowed 1 day of bereavement.

In the event of a death, Employees should make their manager aware of their situation as soon as possible. In turn, the manager should notify HR regarding the reason and length of the Employee's absence. Upon returning to work, the Employee must record his/her absence as a Bereavement Leave on his/her attendance record.

2.6 PARENTAL LEAVE

Maternity Leave and Pay Policy

Employees are entitled to 52 weeks statutory maternity leave regardless of their hours or length of service, whether they work full-time or part-time and whether they are employed on a permanent or temporary basis. The first 26 weeks is known as 'Ordinary Maternity Leave', the last 26 weeks as 'Additional Maternity Leave'.

The earliest that leave can be taken is 11 weeks before the expected week of childbirth unless the baby is born early.

For more information visit:

[Statutory Maternity Pay and Leave: employer guide: Entitlement - GOV.UK \(www.gov.uk\)](#)

Breastfeeding

Employees who continue to breastfeed when they return to work should follow the guidance provided here:

[Continuing to breastfeed when you return to work - Maternity Action](#)

Paternity Leave and Pay

Statutory Paternity Leave is a maximum of two weeks' leave, following the birth of a child, adopting a child, or having a baby through a surrogacy arrangement.

For more information visit:

[Paternity pay and leave: Overview - GOV.UK \(www.gov.uk\)](#)

Shared Parental Leave

You and your partner may be able to get Shared Parental Leave (SPL) and Statutory Shared Parental Pay (ShPP) if you're:

- Having a baby
- Using a surrogate to have a baby
- Adopting a child
- Fostering a child who you're planning to adopt

For more information visit:

[Shared Parental Leave and Pay: How it works - GOV.UK \(www.gov.uk\)](#)

Unpaid Parental Leave

Parental leave is unpaid. You're entitled to 18 weeks' leave for each child and adopted child, up to their 18th birthday.

The limit on how much parental leave each parent can take in a year is 4 weeks for each child (unless the employer agrees otherwise).

You must take parental leave as whole weeks (e.g., 1 week or 2 weeks) rather than individual days, unless your employer agrees otherwise or if your child is disabled. You don't have to take all the leave at once. A 'week' equals the length of time an employee normally works over 7 days.

For more information visit:

Unpaid parental leave: Overview - GOV.UK (www.gov.uk)

Time Off for Dependants

You are legally entitled to take a reasonable amount of time off to deal with certain prescribed emergencies involving certain dependants. This leave is called Time Off for Dependants. A dependant is your child (including adopted child), husband, wife, or parent. It also includes someone who lives in your household, and someone who reasonably relies on you, such as an elderly relative. Any time taken off must be necessary and reasonable in the particular circumstances. Time Off for Dependants is not paid.

For more information visit:

Time off for family and dependants: Your rights - GOV.UK (www.gov.uk)

2.7 EXTRAORDINARY PAID LEAVE

In certain circumstances the company may grant the employee extraordinary leave with or without pay if the circumstances are deemed justifiable by the Employer.

2.8 HOURS OF WORK

Your normal hours and working pattern will be specified in your Contract of Employment. The full-time contracted hours for all posts within the organisation are 37.5 hours per week excluding daily meal breaks. A daily unpaid lunch break of a minimum of 30 minutes must be taken if you work more than six hours daily.

The company reserves the right to vary your hours and pattern of working, following consultation and agreement with you.

3 COMPENSATION

3.1 PAYMENT OF WAGES

Your salary will be paid monthly in arrears by the end of each month by direct credit transfer to your designated bank account.

Your basic pay was outlined in your Contract of Employment. Any subsequent amendments to your basic pay will be notified to you in writing by the Company.

Part-time employees will be paid on a pro rata basis based on the hours they work. In all other aspects, their salaries will be paid in accordance with the pay arrangements for full-time employees of the Company.

If any queries arise with regard to pay speak to Human Resources immediately so that they can take appropriate action. Unless agreed otherwise, any pay errors will be rectified in the next salary payment.

Appropriate deductions will be made from pay including income tax and National Insurance contributions (NICs).

3.2 INCOME TAX

If there are any changes in your personal circumstances which will affect your tax status, you should notify the HM Revenue and Customs (HMRC), who will automatically inform the Company of any changes to your tax code.

For more information visit:

<https://www.gov.uk/tell-hmrc-change-of-details/income-changes>

3.3 EXPENSE REPORTING POLICY AND PROCEDURE

All Employees will be reimbursed for any expenditure necessarily incurred in order to do your job when working away from your normal place of work. Public Transport and accommodation costs will be reimbursed at actual cost – appropriate receipts must accompany all claims. All expense report submissions must follow the Business Travel and Expense Reimbursement Policy.

All charges on Companies' credit cards must be approved. Unauthorized charges on Companies' credit cards can result in disciplinary action.

4 POLICIES

4.1 VERIFICATION OF EMPLOYMENT AND PAID SURVEY'S

Only Human Resources is authorized to acknowledge and respond to requests for employment and salary verifications. If you receive a request, please forward it directly to Human Resources. The Company will verify titles and employment dates; however, for your protection, the Company requires your written authorization before we release any salary or other personal information.

If an employee is contacted to participate in a paid survey regarding the company business, they should immediately notify Human Resources as there may be a conflict of interest and confidentiality concerns.

4.2 OPEN DOOR

To ensure harmonious working relations, the Company believes it is important that issues be resolved before serious problems develop. Most incidents resolve themselves naturally; however, if you and your manager cannot agree on the interpretation of a policy or procedure, you will have an opportunity to discuss your opinion with Human Resources.

4.3 EQUAL OPPORTUNITY

We are an equal opportunity employer and do not discriminate against applicants or Employees on the basis of any protected characteristic.

The Company strives to ensure that all qualified individuals are afforded equal job opportunities and that all Employees receive fair and equal treatment, including but not limited to recruitment, hiring, promotion, compensation, training, layoff, or discharge.

If you believe that you have been subjected to discrimination by any person in connection with your employment with us, you should immediately bring the matter to the attention of your manager. If you feel uncomfortable discussing the incident with your manager, or the incident relates to your manager, notify a member of Human Resources or the executive management team.

All complaints of discrimination will be investigated promptly, and necessary corrective action will be taken. Any investigation of such complaints will be treated as confidential to the extent possible. No Employee will be retaliated against, punished, or suffer any adverse employment action as a result of bringing any good-faith harassment complaint to our attention. If you believe that you have been retaliated against because you reported discrimination or you participated in an investigation into discrimination, you should immediately bring the matter to the attention of your manager, a member of Human Resources, or a member of the executive management team.

Any Employee who is found to have engaged in discrimination or retaliation against an Employee for exercising rights protected by this policy will be subject to the appropriate disciplinary actions. Equally any Employee who knowingly makes a false claim of discrimination may be subject to disciplinary action.

4.4 ANTI-HARASSMENT

It is our Companies' policy that all employment relationships shall be conducted in an environment that is not hostile, intimidating, or offensive. Every Employee, regardless of position, is treated with respect and in a fair and just manner at all times. The Company has zero tolerance for harassment based on an individual's age, race, creed, colour, religion, national origin, sex, gender identity, sexual orientation, disability, or marital status, or any other basis prohibited by law. Harassment includes, but is not limited to:

- **Verbal harassment**, such as making a joke or comment that refers to a certain ethnic group, race, sex, nationality, age, disability, gender identity, sexual orientation, religion or belief, epithets, derogatory comments, vulgar, or profane words and expressions or slurs.
- **Physical harassment**, such as assault and blocking, impairing, or otherwise physically interfering with an individual's normal work or movement.
- **Visual forms of harassment**, such as derogatory photographs, pictures, screen savers, posters, email, cartoons, or drawings.
- **Sexual harassment**, such as unwelcome sexual advances or requests for sexual favours; verbal, visual, or physical conduct of a sexual nature, such as name calling, obscene jokes, sexually suggestive email, or comments or insulting sounds; graphic or verbal comments of a sexual nature about a person's anatomy; or displaying at work sexually suggestive email, photographs, objects, posters, drawings, screen savers, or pictures.

If you believe that you have been subjected to harassment by any person in connection with your employment, you should immediately bring this matter to the attention of your manager. If you feel uncomfortable discussing the incident with your manager, or the incident relates to your manager, notify a member of HR or a member of the executive management team.

All complaints of harassment will be investigated promptly, and necessary corrective action will be taken. Any investigation of such complaints will be treated as confidential to the extent possible. No Employee will be retaliated against, punished, or suffer any adverse employment action as a result of bringing any good-faith harassment complaint to the Companies' attention or for participating in any harassment investigation. If you believe that you have been retaliated against because you reported harassment or participated in an investigation into harassment, you should immediately bring the matter to the attention of your manager, a member of HR, or a member of the executive management team.

Any Employee who is found to have engaged in harassment or retaliation against an Employee for exercising rights protected by this policy will be subject to disciplinary action. Any Employee who knowingly makes a false claim of harassment will also be subject to disciplinary action.

4.5 EMPLOYMENT OF RELATIVES, NEPOTISM, AND NO-FRATERNIZING POLICY

Bamboo wants to ensure that corporate practices do not create situations such as conflict of interest or favouritism. This extends to practices that involve Employee hiring, promotion, and transfer.

To protect the Company from conflict of interest or situations that would give the appearance of conflict of interest because of personal relationships, close relatives, partners, those in a dating relationship, or members of the same household are not permitted to be in positions that have a reporting responsibility to each other.

Close relatives are defined as husband, wife, domestic partner, father, mother, father-in-law, mother-in law, grandfather, grandmother, son, son-in-law, daughter, daughter-in law, uncle, aunt, nephew, niece, brother, sister, brother-in-law, sister-in-law, step relatives, cousins, and domestic partner relatives. Further, managers are not allowed to date Employees of the Company. Romantic involvement between unmarried Employees is prohibited where there is a manager-Employee relationship between the 2 persons involved.

Although the Company does not have a prohibition against employing relatives of current Employees, the Company is committed to monitoring situations in which such relationships exist in the same area. In case of actual or potential problems, the Company will take prompt action.

4.6 DRESS CODE

Dress, grooming, and personal cleanliness standards contribute to the morale of all Employees and affect the professional image our Company presents to our clients and the community. Therefore, the Company wishes to create a positive atmosphere where Employees can work comfortably and creatively.

Listed below are guidelines for acceptable attire, as well as some of the more common items that are not acceptable for the office or client facing virtual meetings.

General dress code requirements:

- Examples of acceptable wear include polo-style shirts, button-down shirts, sweaters/ pull overs, blouses, casual tops, jeans (without holes/tears) casual pants, casual leather shoes, clean sneakers, dressy sandals.
- Unacceptable attire: short skirts, shorts, sweatpants/shirts, flip flops, t-shirts, workout attire, spaghetti straps, pyjamas, or crop tops.

If you report for work or join a virtual meeting with inappropriate attire, it is our policy that your manager may discreetly ask you to return home and/or change into clothing suitable for meeting these dress code requirements.

4.7 INCLEMENT WEATHER AND EMERGENCY CLOSING

While the majority of our workforce are remote workers, we recognize your concerns about traveling on days of inclement weather and are delegating the responsibility to each Employee for your own safety. If you feel that existing or predicted weather conditions are serious enough to warrant working from home, you are to notify your manager and provide an explanation of the situation.

We request that each Employee weigh the decision with their personal safety in mind and with equal consideration for the Company.

It is expected that Employees will plan ahead and make provisions to limit the amount of time not worked because of office closing in relation to inclement weather (e.g., bringing laptops home when inclement weather is predicted).

4.8 BACKGROUND AND CREDIT SCREENING

All Employees that the Company considers for employment may be required to submit to a background screening. This is only in very special circumstances where your employment with us means you are likely to come into contact with sensitive information. Should this be the case, we will discuss the situation with you prior to confirming your appointment (or relevant change to your job).

4.9 NON-DISCLOSURE/CONFIDENTIALITY

The protection of confidential business information and trade secrets is vital to the interests and the success of the Company. Such confidential information includes, but is not limited to, the following examples:

- New research materials
- Business plans
- Customer lists and data
- Proprietary IT systems and processes
- Pending projects and proposals
- Proprietary production processes
- Research and development strategies
- Corporate data
- IT or scientific formulae

Employees who improperly use or disclose trade secrets or confidential business information will be subject to disciplinary action, even if they do not actually benefit from the disclosed information.

4.10 CONTACT WITH THE MEDIA

Only those Employees specifically authorized are allowed to communicate with representatives of the media (television, radio, newspapers, publications, etc.). If the media contacts you, and you have not been given prior authorization to communicate with the media, immediately refer all inquiries to Human Resources.

4.11 CONTINUING EDUCATION

You may be eligible for reimbursement up to 800 GBP annually for continuing education seminars and/or courses that are job related and help you perform your job better. Refer to the Education Assistance Program or contact Human Resources for more information.

4.12 CONTRACTS

Employees are prohibited from entering into any contracts or agreements on behalf of the Company through email or any other means. Any such contracts or agreements must be executed by either the group CEO or CFO.

4.13 PERSONNEL RECORDS

Your personnel records are treated as confidential. Additional information about you, your salary or job history will not be released without your written or documented authorization, unless otherwise required by law.

Keeping the information in your personnel records up to date will prevent administrative errors and help accuracy in benefit administration. Please notify Human Resources when any of the following changes occur:

- Name
- Address
- Telephone number
- Emergency notification number

For more information visit:

[Your right of access | ICO](#)

4.14 SICK PAY PROVISION

Statutory Sick Pay (SSP)

Most employees have a right to statutory sick pay (SSP) as long as they earn more than the lower earnings level. SSP is not however payable for the first four qualifying days of absence (a qualifying day is a day on which you are normally expected to work under your contract of employment).

There is a limit of 28 weeks' SSP in any one period of sickness or linked periods (periods of sickness are said to be linked if the second period starts within eight weeks of the end of the first period). SSP is paid in the same way as ordinary pay and is liable to tax and National Insurance contributions.

4.15 FIT FOR DUTY

In effort to help ensure that Employees are able to perform their duties safely, certain Employees, on the basis of job requirements, may be required to take medical examinations to determine fitness for duty. Such initial and potentially recurring examinations will be scheduled at reasonable times and intervals and performed at the Companies' expense.

Where appropriate, an Employee who is returning from long term sick leave, or other medical-related leaves of absence may be required to provide a certification from their physician stating that they are fit to perform the duties of their position.

4.16 RETURN OF PROPERTY

You are responsible for all company property, materials, or written information issued to you or in your possession or control during your employment. In the event your employment is terminated, you must return the Companies' property on or before your last day of work. If property is returned damaged by the employee the Company, where permitted, may hold the employee responsible to pay for such damages.

4.17 SOLICITATION

To ensure a productive and harmonious work environment, people not employed by our Company may not solicit or distribute literature in the workplace at any time for any purpose.

We recognize that Employees may have interests in events and organizations outside the workplace. However, Employees may not solicit or distribute literature concerning these activities during working time. Working time does not include lunch periods, work breaks, or any other periods in which Employees are not on duty.

In addition, the posting of written solicitations on company bulletin boards is prohibited. Bulletin boards are reserved for official company communications.

4.18 OUTSIDE EMPLOYMENT

You may hold a job with another organization as long you satisfactorily perform your job responsibilities with the Company. All Employees will be judged by the same performance standards and will be subject to Companies' scheduling demands, regardless of any existing outside work requirements.

If the Company determines that an Employee's outside work interferes with performance or the ability to meet the requirements of our Company as they are modified from time to time, you may be asked to terminate the outside employment if you wish to remain employed with the Company.

Employees are encouraged to discuss any potential outside employment with their manager or Human Resources to ensure transparency and compliance with company policies, as outside employment may have implications on conflicts of interest and time management. Employees are prohibited from outside employment that presents a conflict of interest or has a negative impact on the Company.

4.19 EMPLOYEE CONDUCT AND WORK RULES

To ensure orderly operations and provide the best possible work environment, the Company expects Employees to follow rules of conduct that will protect the interests and safety of all Employees and the organization.

It is not possible to list all the forms of behaviour that are considered unacceptable in the workplace. The following are examples, but not an all-inclusive list of infractions of rules of conduct that may result in disciplinary action, up to and including termination of employment:

- Theft or inappropriate removal or possession of property
- Falsification of timekeeping records and other employment records
- Working under the influence of alcohol or illegal drugs
- Possession, distribution, sale, transfer, or use of alcohol or illegal drugs in the workplace, while on duty, or while operating employer-owned vehicles or equipment
- Fighting or threatening violence in the workplace
- Boisterous or disruptive activity in the workplace
- Negligence or improper conduct leading to damage of employer-owned or customer-owned property
- Insubordination or other disrespectful conduct
- Violation of safety or health rules
- Smoking in prohibited areas
- Sexual or other unlawful or unwelcome harassment
- Possession of dangerous or unauthorized materials, such as explosives or firearms, in the workplace
- Excessive absenteeism or violation of the Attendance and Punctuality policy
- Unauthorized absence from work during the workday
- Unauthorized use of telephones, mail system, or other employer-owned equipment
- Unauthorized disclosure of business “secrets” or confidential information
- Violation of personnel policies
- Unsatisfactory performance or conduct

4.20 BUSINESS ETHICS AND CONDUCT

The successful business operation and reputation of our Company is built upon the principles of fair dealing and ethical conduct of our Employees. Our reputation for integrity and excellence requires careful observance of the spirit and letter of all applicable laws and regulations, as well as a scrupulous regard for the highest standards of conduct and personal integrity.

We are placing trust in you to behave responsibly and use good judgment in using Companies’ resources. Company resources, including the Companies’ time, material, equipment, and information, are provided for the Companies’ business use. Occasional personal use of company resources by Employees may occur without adversely affecting the interests of the Company. Personal use of company resources must not result in significant added costs, disruption of business processes, or any other disadvantage to the Company. Use of company resources for non-company purposes is appropriate only when specifically authorized by policy or procedure, or when you receive express authorization to do so from your manager.

Our continued success is dependent upon our customers’ trust and the Company is dedicated to preserving that trust. Employees owe a duty to the Company, their customers, and shareholders to act in a way that will merit the continued trust and confidence of the public.

We will comply with all applicable laws and regulations and expect all directors, officers, and Employees to conduct business in accordance with the letter, spirit, and intent of all relevant laws and to refrain from any illegal, dishonest, or unethical conduct.

In general, the use of good judgment, based on high ethical principles, will guide you with respect to lines of acceptable conduct. If a situation arises where it is difficult to determine the proper course of action, the matter should be discussed openly with your manager, and, if necessary, with any of the HR staff for advice and consultation.

Customers are among our organization's most valuable assets. Every Employee represents the Company to our customers and to the public. The way the Company works presents an image of our entire organization. Customers judge all of us by how they are treated with each Employee contact. Therefore, one of our first business priorities is to assist any customer or potential customer. Nothing is more important than being courteous, friendly, helpful, and prompt in the attention you give to customers.

Our personal contact with the public, our manners on the telephone, and the communications the Company sends to customers are a reflection not only of ourselves, but also of the professionalism of the Company. Positive customer relations not only enhance the public's perception or image of the Company, but also pay off in greater customer loyalty and increased sales and profit.

Compliance with this policy of business ethics and conduct is the responsibility of every Employee.

4.21 DISCIPLINARY PROCEDURE

The Company strives to administer equitable and consistent discipline for unsatisfactory conduct in the workplace. The best disciplinary measure is one that does not have to be enforced and comes from good leadership and fair supervision at all employment levels.

The Companies' best interests lie in ensuring fair treatment of all Employees and in making certain that disciplinary actions are prompt, uniform, and impartial. The major purpose of any disciplinary action is to correct the problem, prevent recurrence, and prepare the Employee for satisfactory service in the future.

Disciplinary action may call for any of 4 steps: verbal warning, written warning, suspension with or without pay, or termination of employment, depending on the severity of the problem and the number of occurrences. There may be circumstances when 1 or more steps are bypassed.

Progressive discipline means that, with respect to many disciplinary problems, these steps will normally be followed: a first offense may call for a verbal warning, a next offense may be followed by a written warning, another offense may lead to a suspension, and still another offense may then lead to termination of employment.

We recognize that there are certain types of Employee problems that justify either a suspension or termination of employment, without going through the sequential progressive discipline steps.

While it is impossible to list every type of behaviour that may be deemed a serious offense, this Handbook includes examples of problems that may result in immediate suspension or termination of employment. However, the problems listed are not all necessarily serious offenses, but may be examples of unsatisfactory conduct that will trigger progressive discipline.

By using progressive discipline, the Companies hope that most Employee problems can be corrected at an early stage, benefiting both the Employee and the Company.

While it is impossible to list every type of behaviour that may be deemed a serious offense, the following are some examples of conduct that are grounds for immediate dismissal of an Employee:

- Breach of trust or dishonesty
- Conviction of a felony that negatively impacts your ability to perform essential job duties or creates a health or safety risk
- Wilful violation of an established policy or rule
- Falsification of company records
- Gross negligence
- Insubordination
- Violation of the Anti-Harassment and/or Equal Employment Policies
- Undue and unauthorized absence from duty during regularly scheduled work hours
- Deliberate non-performance of work
- Possession of dangerous weapons on the premises
- Marring, defacing, or other wilful destruction of any supplies, equipment, or property of the Companies
- Fighting or serious breach of acceptable behaviour
- Violation of the Alcohol or Drug Policy
- Theft
- Violation of the Companies' Conflict of Interest/Outside Employment Policy, Business Ethics and Conduct, and/or Confidentiality Policy

4.22 PERFORMANCE EVALUATION & MANAGEMENT, CAREER DEVELOPMENT

Managers and Employees are strongly encouraged to discuss job performance and goals on an informal and ongoing basis.

Merit-based pay adjustments will be awarded in an effort to recognize truly superior Employee performance. The decision to award such an adjustment is dependent upon numerous factors, including the information documented by the Companies' formal performance evaluation process.

We also strongly encourage all Employees to continue learning and developing their workplace skills, whether in cross-training with internal job training opportunities, or off-site with career development opportunities. Whether voluntary or required for certain positions, the Company recognizes that doing so can increase the Employee's understanding of various tasks and departments while enhancing their own career development.

PERFORMANCE MANAGEMENT

All Bamboo Employees will participate in the company annual performance management procedure. Individual performance goals will be defined in conjunction with the Employee's direct manager and at the end of the year during the year-end review. Regular, ongoing feedback on performance and goal attainment is encouraged year-round.

4.23 CONFLICT OF INTEREST

The Company expects you to conduct yourself, at all times, in a manner consistent with the best interests of your colleagues, your department, and the Company. This applies particularly to association with other Employees at all levels and with customers, competitors, and vendors. You should avoid personal activities or involvement from which personal benefit or obligation may potentially result, create, or appear to others to create a conflict with your responsibility, loyalty, and the welfare of the Company. Other employment, including freelancing, consulting, etc., must not interfere with your ability to perform your duties and fulfil your obligations to the Company, and there must be no conflict of interest.

4.24 ACCEPTANCE OF GIFTS

No Employee may solicit or accept gifts of significant value (i.e., in excess of 25.00 GBP), lavish entertainment, or other benefits from potential and actual customers, suppliers, vendors or competitors. Special care must be taken to avoid even the impression of a conflict of interest.

An Employee may entertain potential or actual customers if such entertainment is consistent with the Bamboo's Compliance Policy, accepted business practices, does not violate any law or generally accepted ethical standards, and the public disclosure of facts will not embarrass the Company. Any questions regarding this policy should be addressed to the HR Department.

4.25 WORK PRODUCT OWNERSHIP

All Employees must be aware that the Company retains legal ownership of the product of Employee's work. No work product created while employed with the Company can be claimed, construed, or presented as property of the Employee, even after employment with the Company has been terminated or the relevant project completed. "Work product" includes written and electronic documents, audio and video recordings, system code, and also any concepts, inventions, ideas, or other intellectual property developed for the Company, regardless of whether the intellectual property is actually used by the Company. In any event, it must always be made clear that work product is the sole and exclusive property of the Company. Freelancers, contract Employees, and temporary Employees must be particularly careful in the course of any work they discuss doing, or actually do, for a competitor of the Company and are held to the same confidentiality requirements as the full-time and part-time Employees of the Company.

4.26 REMOTE WORKING POLICY/FLEXIBLE WORKING POLICY

In an effort to foster flexibility among our workforce, Bamboo has instituted a comprehensive remote working/flexible working policy. While remote/flexible work is considered a viable and flexible option, it is crucial to note that it is not an entitlement, and it does not alter the existing terms and conditions of employment with Bamboo.

Eligibility

All employees are eligible for the remote/flexible working option, provided that the nature of their job duties allows for it. Certain roles may be required to work from the office based on business needs and management requests. The expectation is that employees working remotely will remain available and attend all meetings during regular working hours. The overarching goal is to offer flexibility while ensuring the company's operational needs are met.

Security

Remote employees are expected to uphold the same information security standards as those working in the office. This includes safeguarding proprietary company and customer information accessible from their home office through measures such as locked file cabinets, secure desks, regular password maintenance, and any other relevant security protocols.

Safety

Employees are responsible for maintaining a safe home workspace free from hazards. In the event of injuries related to regular work duties in a home office, the company's Employers Liability Insurance policy applies.

Remote employees must promptly report such injuries to Human Resources. Employees are responsible for any injuries sustained by visitors to their home worksite.

Childcare

Remote work is not a substitute for proper childcare. While an employee's schedule may be adjusted to accommodate childcare needs, the primary focus must remain on job performance and meeting business demands. Regular care of an infant child during working hours is not permissible, excluding situations involving sick children.

To ensure operational consistency, remote employees located in a particular jurisdiction are required to obtain company approval before relocating to a different jurisdiction (other than where originally hired).

4.27 COMPANY EQUIPMENT

The Company will provide all Employees with the standard equipment and materials necessary to perform their job. These items are to be used solely for the Companies' purposes. Employees are expected to exercise care in the use of company equipment and property and use such property only for authorized purposes. Loss, damages, or theft of company property should be reported at once. The Company does not permit the use of personal computers to be used for company-related or client-related work. Upon termination of employment, the Employee must return all company property, equipment, work product, and documents in their possession or control in proper working order.

The Employee is responsible for any IT equipment or property issued to them and for any damage that is a direct result of neglect (excluding normal wear and tear).

4.28 ENVIRONMENTAL POLICY

Bamboo is committed to providing quality service in a manner that ensures a safe and healthy workplace for our Employees and minimizes our potential impact on the environment. At the same time, we recognize that building a resilient, sustainable company of the future requires a proactive approach to considering environmental, social and governance (ESG) matters in our business. The Company will operate responsibly and in compliance with all relevant environmental legislation and the Company's ESG policy. We will strive to use pollution prevention and environmental best practices in all the company functions.

We will:

- Integrate the consideration of environmental concerns and impacts into all our decision-making and activities
- Promote environmental awareness among our Employees and encourage them to work in an environmentally responsible manner
- Train, educate, and inform our Employees about environmental issues that may affect their work
- Reduce waste through reuse and recycling and by purchasing recycled, recyclable, or refurbished products and materials where these alternatives are available, economical, and suitable
- Promote efficient use of materials and resources throughout our facilities including water, electricity, raw materials, and other resources, particularly those that are non-renewable
- Avoid unnecessary use of hazardous materials and products, seek substitutions when feasible, and take all reasonable steps to protect human health and the environment when such materials must be used, stored, and disposed of
- Purchase and use environmentally responsible products accordingly
- Where required by legislation or where significant health, safety, or environmental hazards exist, develop and maintain appropriate emergency and spill response programs

- Communicate our environmental commitment to clients, customers, and the public and encourage their support
- Strive to continually improve our environmental performance and minimize the social impact and damage of activities by periodically reviewing our environmental policy in light of our current and planned future activities

4.29 WHISTLEBLOWER POLICY

This Whistleblower Policy is to encourage employees to report any unethical, illegal, or fraudulent activities within the organization and to protect individuals who make such reports from retaliation. This policy outlines the procedures for reporting concerns and the steps the company will take to investigate and address reported issues.

Scope:

Applies to all individuals associated with Bamboo, including employees, contractors, and consultants.

Reporting Mechanisms:

Employees can report concerns to their manager, Human Resources, or through the anonymous hotline at 001-855-252-7606.

Protections Against Retaliation:

Retaliation against whistleblowers is strictly prohibited, and any such incidents will be promptly investigated.

Confidentiality:

Reports will be treated with utmost confidentiality, disclosed only to individuals necessary for investigation, and in compliance with applicable laws.

Investigation Process:

All reports will be thoroughly investigated, and appropriate actions will be taken if misconduct is identified.

No Reprisals:

Employees reporting concerns in good faith will not face reprisals or adverse employment actions.

Review and Updates:

This policy will be periodically reviewed to ensure effectiveness and compliance with laws and regulations.

By adhering to this Whistleblower Policy, Bamboo fosters transparency and ethical conduct, allowing employees to speak up without fear of reprisal.

4.30 DATA SECURITY AND PRIVACY POLICY

Bamboo must protect all company confidential or sensitive data from loss to avoid reputation damage and adversely impacting our business. We must also gather and use certain information about individuals including suppliers, consultants, clients, employees, and other people the company has a relationship with or may need to contact. The protection of data is a critical business requirement, yet flexibility to access data and work effectively is also critical. It is not anticipated that these processes can effectively deal with all malicious theft

scenarios, or that it will reliably detect all data. Its primary objective is user awareness and to avoid accidental data loss scenarios.

Data security policies describe how data must be collected, handled, and stored appropriately to meet the Companies' data security standards—and to comply with corporate and global regulations, whether said data are collected on paper, stored in a computer database, or recorded on other material.

Data protection policies ensure Bamboo:

- Complies with data protection laws, including the General Data Protection Regulation (GDPR), if applicable, and follows good practice
- Protects the rights of employees, customers, and partners
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

Devices in scope:

- Any device that handles company data, network member data, client data, sensitive data, or personally identifiable information, including any such device used by Remote Employees
- Any device that is regularly used for email, web, or other work-related tasks and is not specifically exempt for legitimate business or technology reasons, including any such device used by Remote Employees

Data in scope:

- Business development including client data
- Account services
- Axxess Network
- Client owned
- Scientific/clinical
- Marketing
- Creative design
- IT
- HR
- Financial
- Legal

Data Loss Protection

Electronically stored data must be protected from unauthorized access, accidental deletion, and malicious hacking attempts within the approved Bamboo IT ecosystem.

- The only people able to access data are those who need it for their work. Bamboo manages this by restricting access to SharePoint groups, folders, email distros, and systems
- Bamboo's data security policy will scan for data in motion. Our data loss protection (DLP) technology will identify large volumes of any in-scope data/files being sensitive and likely to have significant impact if handled inappropriately
- Exports of any company identifiable information outside Bamboo controlled systems will be automatically flagged to the IT department for review
- DLP will log incidents centrally for review. The IT team will conduct first-level triage on events, identifying data that may be sensitive and situations where its transfer was authorized and there is a

concern of inappropriate use. These events will be escalated to the employee's manager and HR if necessary

- Where there is an active concern of a data breach, the IT department will immediately report the incident and resolution processes to be used with specific notification provided to the executive team
- Access to DLP events will be restricted to the IT department to protect the privacy of employees. A DLP event does not constitute evidence that an employee has intentionally or accidentally lost data, but provides enough basis for investigation to ensure data have been appropriately protected

Employee Requirements

- Everyone who works for or with Bamboo has a responsibility for ensuring data are collected, stored, and handled appropriately within our approved IT ecosystem
- Each team member who handles data (including personal data of EU data subjects) must ensure that the data are handled and processed in line with the data security policy and data protection principles, and must comply with the Bamboo GDPR Compliance Policy (and all exhibits included in the policy), attached to this Employee Handbook as Attachment A.
- Each team member who handles personal data of EU data subjects is also required to review the Bamboo GDPR Compliance policy (Attachment A) as part of their initial staff induction training and will receive regular data protection training and procedural guidance. Any questions regarding such policies should be directed to the Chief Privacy Officer
- Email spam filtering technology is employed in our IT ecosystem. However, all team members do have a responsibility to act as a human firewall. This includes regular management of individual email account spam filter and junk mailbox to ensure that messages are delivered or blocked appropriately. All data must be stored on Bamboo's approved SharePoint or One Drive(s). Any storage of data on third party file applications such as Google, Dropbox, or other is a direct violation of the company's data security policy
- Saving files directly to a laptop or other mobile devices such as tablets or smartphones should be avoided. When unavoidable, only store highly necessary information, and remove data from devices as soon as possible
- If any files are stored on a laptop, ensure a back-up to One Drive is made monthly to avoid data being lost if the laptop is damaged or lost
- When working with data, employees should ensure access to their computer, smartphone, and/or tablet is always locked when the device is left unattended. Devices should be set to lock automatically if inactive for 5 minutes
- Sensitive/confidential data should be protected by strong passwords. This is particularly important for confidential documents, such as presentations or files that have personal data. Many file types can be password-protected easily. When transferring such documents, remember not to send the password in the same email as the document
- Do not use sticky notes with login information on or around your device. Keep your login information stored elsewhere
- Strong passwords are to be used on your laptop, mobile phone, and tablet, and they should never be shared. Passwords on company laptops will expire every 60 days and the last 10 passwords cannot be re-used
- You are required to not reference the subject or content of sensitive or confidential data publicly or via systems or communication channels not controlled by Bamboo. For example, the use of external email systems not hosted by Bamboo to distribute data is not allowed
- When sending emails to clients, double check the distribution list before sending to avoid emails accidentally being sent to the wrong recipient (e.g., a competitor client with a similar first or last name)

- Do not use the “remember username and password” option that many internet browsers provide. Always log out of websites that require a login, and keep your login details stored safely
- When onsite for a project, or in an area where unauthorized persons can view your screen, it is advised to use a privacy screen on your laptop to avoid direct line of sight to the information on your screen.
- When in meetings with clients (e.g., on site, WebEx), disable pop ups and alerts (e.g., Outlook, Teams)
- Data should not be shared informally. When access to confidential information is required, Employees can request it from their managers
- Personal data should not be disclosed to unauthorized people, either within the company or externally
- Data should be regularly reviewed and updated if the data are found to be out of date. If it is no longer required or necessary to achieve the purposes for which such data were collected and are being processed, data should be deleted and disposed of. Information will be stored only if it is needed to achieve the purpose for which such data were collected and are being processed or required by statute and will be disposed of appropriately
- Immediately notify the IT department if a device containing in-scope data is lost (e.g., mobile phone, laptop)
- Data that must be moved within Bamboo are to be transferred only via business-provided secure transfer mechanisms (SharePoint, email, etc). Bamboo will provide you with systems or devices that fit this purpose. You must not use other mechanisms to handle in-scope data. If you have a query regarding use of a transfer mechanism or it does not meet your business purpose, you must raise this with the IT department
- If you find a system or processes that you suspect are not compliant with this policy or the objective of information security, you have a duty to inform the IT department so that they can take appropriate action
- Employees will be required to return all data containing company information in any format prior to exit from employment at Bamboo

Data stored on paper should be kept in a secure place, away from potential unauthorized viewers. These guidelines also apply to data that are usually stored electronically but have been printed out for some reason.

- When not required, the paper or files should be kept in a (locked) drawer or filing cabinet
- Employees should make sure paper and printouts are not left where unauthorized people could see them, such as on a printer or in a hotel (meeting) room
- Data printouts should be shredded and disposed of securely when no longer required. Shredders and locked paper disposal containers are provided in the office where applicable.

It is Bamboo 's responsibility to:

- Ensure that all local and cloud servers and computers containing data are protected by approved security software
- Ensure all personal and company data are non-recoverable from any computer system previously used within the organization that has been passed on/sold to a third party
- Ensure that servers containing personal data are sited in a secure location, away from general office space
- Back up data on Office 365 (Outlook, One Drive) and SharePoint. Back-ups should be tested regularly, in line with the companies' standard back-up procedures
- Provide training to all employees to
 - Help them understand their responsibilities when handling data, including compliance with applicable laws, including the GDPR
 - Ensure that everyone processing personal information understands that they are contractually responsible for following good data protection practice

- Ensure that all staff are aware that a breach of the rules and procedures identified in this policy may lead to disciplinary action being taken against them

Employees should request help from their manager, the Chief Privacy Officer, or IT department if they are unsure about any aspect of data protection.

5 WORKPLACE SAFETY

To provide a safe and healthful work environment for our Employees, our customers, and our visitors, the Company has set workplace safety as a top priority. The Company is responsible for implementing, administering, and evaluating safety in the workplace. The Company believes our safety success depends on the alertness and personal commitment of all.

Some of the best safety improvement ideas come from our Employees. If you have ideas, concerns, or suggestions for improved safety in the workplace, Employees are encouraged to raise them with their manager. Reports and concerns about workplace safety issues may be made anonymously, and all reports can be made without fear of reprisal.

For more information visit:

[HSE: Information about health and safety at work](#)

5.1 CONTROLLED SUBSTANCES

Our Employees are our most valuable resource. The Company cannot have a safe and productive work environment if anyone is under the influence of alcohol or drugs. Therefore, the Company is opposed to any situation where the use of alcohol or drugs interferes with any Employee's health or job performance, poses a safety problem, adversely affects the job performance of any Employee, or is considered detrimental to the Companies' business.

Arriving on company premises or working under the influence of any illegal drug or alcohol is strictly prohibited. Also prohibited are the use, sale, purchase, transfer, or possession of illegal drugs, or the unauthorized or illegal use, sale, purchase, transfer, or possession of prescription medications by an Employee on company time.

A violation of any rule in this section subjects the Employee to disciplinary action, up to and including termination.

Legal Drugs and Alcohol

It is strictly prohibited in the work environment to use or be under the influence of any legally obtained drug that adversely affects the job performance of the Employee or any other Employee, poses a safety threat, or is detrimental to the Companies' business. This covers, but is not limited to, arriving on company property under the influence of any legally obtained drug, including any prescribed drug under medical direction, which has the aforementioned effect(s).

It is your responsibility to inform your manager if you believe there is a possibility that the use of any prescription drug may alter your ability to safely perform your assigned tasks. The company will endeavour to support the employee in looking at reasonable adjustments and/or other solutions.

Illegal Drugs

Illegal drugs include (a) drugs that are not legally obtainable; (b) drugs that are legally obtainable but are being handled abusively or illegally; and (c) drugs that are legally obtainable but have not been obtained legally. This definition applies to any forms of narcotics, depressants, stimulants, or hallucinogens whose sales, purchase, possession, transfer, or use are prohibited or restricted by law.

The sale, purchase, transfer, use, or possession of any illegal drug or alcohol by any Employee on company property, in company vehicles, while on company business, while working, or while on break is strictly prohibited.

5.2 DRUG TESTING

Drug testing may be required when circumstances exist that could be indicative of substance abuse and are reasonable cause for suspicion, such as:

- Upon returning from a voluntary medical leave of absence where the Employee sought rehabilitation
- Whenever the Employee's observed behaviour or involvement in an on-the-job accident raises any question about the Employee's physical condition or fitness to perform the Employee's assigned tasks
- After being found selling, purchasing, transferring, possessing, using, or being under the influence of any illegal drug
- After being found while on duty using or being under the influence of any legal drug that has the effects of either interfering with any Employee's health or job performance, posing a safety problem, adversely affecting the job performance of any Employee, or is considered detrimental to company business

We will obtain consent from the employee before any test is conducted. While Employees can't be made to take a drug test, if they refuse when the Employer has good grounds for testing, they may face disciplinary action.

5.3 SMOKING

In keeping with the intent to provide a safe and healthful work environment, smoking (including the use of a vaporizer) is prohibited throughout the workplace. This policy applies equally to all Employees, customers, and visitors. The Company will provide designated smoking areas in alignment with local facility policies.

5.4 WORKPLACE VIOLENCE

We have a strong commitment to providing a safe, healthy, and secure work environment to each of our Employees. While the Company has no intention of intruding into the private lives of present or potential Employees, the Company expects all Employees to report to work without possessing weapons and to work without violence toward any other individual. The Company expects Employees to work in such a manner so that they can perform their duties in a safe and productive manner. Therefore, the Company considers compliance with this policy as a condition of continued employment, and a violation of this policy will result in disciplinary action.

Workplace violence is, among other things, any intentional conduct that is sufficiently severe, offensive, or intimidating to cause an individual to reasonably fear for their personal safety or the safety of their family, friends, and/or property, such that employment conditions are altered, or a hostile, abusive, or intimidating work environment is created.

5.5 EMPLOYERS LIABILITY INSURANCE

In case of accidents that result in injury, regardless of how insignificant the injury may appear, you should immediately notify your manager or HR staff. Such reports are necessary to comply with the conditions of the Employers Liability Insurance.

6 ELECTRONIC DEVICES

6.1 GENERAL

Our electronic and technical resources, including, but not limited to, desktop and portable computer systems, fax machines, internet, and World Wide Web (web) access, voicemail, email, electronic bulletin boards, and our intranet, enable Employees to quickly and efficiently access and exchange information throughout the Company and around the world. All such resources including hardware, software, networks, and communication systems and data are the sole and exclusive property of the Company. Employees have no right of privacy as to any information or file maintained in or on company property or transmitted or stored through company property (owned or leased), including, but not limited to, a company's computer, server, network, voicemail, email, or telephone system.

We have provided technical resources for the benefit of the Company and their customers, vendors, and suppliers. These resources are provided for use in the pursuit of the Companies' business and are to be reviewed, monitored, and used only in that pursuit.

Our technical resources are to be used only for work purposes.

6.2 TELEPHONES AND PERSONAL ELECTRONICS

Proper communication is essential at the Company. The Company recognizes that occasionally it is necessary for employees to make or receive personal telephone calls during working hours. The Company asks that Employees restrict personal telephone usage to emergency situations. Personal long-distance calls may not be charged to the Company. Excessive personal telephone usage may result in progressive discipline.

Violations of this policy may lead to disciplinary action, up to and including employment termination.

The Company recognizes that most mobile phones can take photographs. Because this capability could allow for theft of trade secrets or expose confidential information, you are prohibited from taking photographs of such confidential information.

We also prohibit the use of a hand-held cell phone or other such personal communications device while driving for company purposes.

Voicemail

Every Employee is responsible for using the voicemail system properly and in accordance with this policy.

The voicemail system is the property of the Company. It has been provided for use in the conduct of company business. All communications and information transmitted by, received from, or stored in this system are company records and property of the Company.

The Company, in their discretion as owners of the voicemail system, reserves and may exercise the right to monitor, access, retrieve, and delete any matter stored in, created, received, or sent over the voicemail system, for any reason without the permission of any Employee and without notice.

Even if Employees use a password to access the voicemail system, the confidentiality of any message stored in, created, received, or sent from the Companies' voicemail system still cannot be assured. Use of passwords or other security measures does not in any way diminish the Companies' rights to access materials on their system or create any privacy rights of Employees in the messages and files on the system.

Even though the Company reserves the right to retrieve any voicemail messages, those messages should still be treated as confidential by other Employees and accessed only by the intended recipient. Employees are not authorized to retrieve or listen to any voicemail messages that are not sent to them. Any exception to this policy must receive prior approval from Human Resources.

The Companies' policies against sexual or other harassment apply fully to the voicemail system, and any violation of those policies is grounds for discipline up to and including termination. Therefore, no voicemail messages should be created, sent, or received if they contain intimidating, hostile, or offensive material concerning race, colour, religion, sex, gender identity, sexual orientation, age, national origin, disability, or any other classification protected by law.

The voicemail system may not be used to solicit for religious or political causes, commercial enterprises, outside organizations, or other non-job-related solicitations.

Users should routinely delete outdated or otherwise unnecessary voicemails. These deletions will help keep the system running smoothly and effectively, as well as minimize maintenance costs.

Employees are reminded to be courteous to other users of the system and always to conduct themselves in a professional manner. Voicemails are sometimes misdirected or forwarded and may be heard by people other than the intended recipient. Users should create voicemail communications with no less care, judgment, and responsibility than they would use for letters or internal memoranda written on company letterhead.

The Company has the right to modify this policy at any time, with or without notice.

6.3 COMPANY MOBILE POLICY

There is no legal requirement or obligation for the Company to provide mobile phones to employees.

Company mobile phones are provided to Employees who meet the following criteria:

- Senior Management
- Have a legitimate business need
- Employees who travel for business purposes

There will be no reimbursement of costs associated with personal mobile phones, unless explicitly approved and confirmed in writing.

This policy applies to all holders of company mobile phones and any Employees who become eligible to hold company mobile phones.

- 1) Employees who hold company mobile phones/mobile Wi-Fi devices are reminded that the mobile phone hotspot is company property and ultimate liability for its misuse rests with the user and not with the Company. Calls made or text messages/images sent from the mobile phone are to be treated in the same way as email technology. In other words, Employees should not access, store, or distribute any offensive or inappropriate material with the mobile phone. Non-adherence to this rule will carry serious consequences, up to and including dismissal.
- 2) The number of calls made should be limited to those necessary for effectively conducting business and the calls should be brief.
- 3) When travelling abroad on business, Employees should contact IT before departing to ensure the appropriate international plans are activated to ensure unnecessary charges. Employees should be mindful that roaming charges vary considerably and are generally expensive. Every effort should be made to minimize costs during that time.
- 4) International calls to or from a mobile phone in general should be limited where possible, because of their high expense.

- 5) Employees may be asked to justify monthly bills or individual itemized charges.
- 6) The Company reserves the right to deduct from payroll any phone charges that appear unreasonable, or in excess of an appropriate monthly amount.
- 7) Company-sponsored mobile phones should not be used for text messaging except for business purposes. Employees may be asked to justify the charges apportioned to text messages on the monthly bill.
- 8) Only incidental personal use is allowed.
- 9) Company email accounts should be on company phones only and not on personal mobile phones.
- 10) Extreme care should be exercised when using mobile phones in cars. Mobile phones can only be used in cars when connected to a "hands-free" unit. Using a hand-held mobile device while driving is not permitted by the Company, as it is considered a serious risk and constitutes a legal offence under road traffic legislation in most countries and states. Each Employee is responsible for following all laws in the country state they are in related to hands-free or distracted driving.
- 11) Mobile phone manufacturers' manuals contain safety and operating instructions, which should be read and adhered to at all times. Manuals and user guidelines can be found online or a copy of them can be requested from the person responsible for issuing mobile phones in the Company.
- 12) Mobile phones should be kept charged at all times to ensure that they are fully operational.
- 13) Mobile phones must be kept switched on at all times during working hours and kept in the Employee's possession. They are not to be left in a car when the car is unattended and should not be switched off, except when necessary. While in meetings, mobile phones should be switched to silent mode so as not to disrupt proceedings.
- 14) The phone's message minder (voicemail) must be activated at all times.
- 15) Reasonable care must be taken to prevent accidental damage, loss, or theft of mobile phone/hotspot equipment. In the event of the theft or loss of a mobile phone/hotspot device, the user must immediately notify the person responsible for issuing mobile phones in the Company, who will then contact the network operator to have the phone/hotspot disabled.
- 16) Failure by an individual to adhere to these procedures may result in action being taken to withdraw from the mobile phone facility. Serious or persistent breaches of this policy may result in disciplinary action up to and including dismissal.

6.4 COMPUTER AND INTERNET

At any time and without prior notice, the Company reserves the right to examine email, personal file directories, and other information stored on company computers. The Company may monitor access to the internet; use of the internet constitutes acceptance of such monitoring.

This policy should be read and interpreted in conjunction with all other company policies including, but not limited to, policies prohibiting harassment, discrimination, offensive conduct, or inappropriate behaviour. Employees are prohibited from accessing the internet for any unethical purposes, including pornography, violence, gambling, racism, harassment, or any illegal activity. Employees are forbidden from using profanity or vulgarity when posting email via the internet or posting to public forums (e.g., newsgroups). Any email sent through or postings to public forums must fall within these ethical standards.

6.5 SOFTWARE DOWNLOADS

Employees are prohibited from downloading software from the internet without prior written approval from your manager or IT. Downloading games from the internet is prohibited. Downloading of any executable files or programs that change the configuration of your system by anyone other than the IT Department is prohibited. If your request to download files or programs from the internet is approved, you should take extreme caution when downloading. All files or software should be passed through virus protection programs prior to use. Failure to detect viruses could result in corruption or damage to files and/or unauthorized entry into the

Companies' network. It is mandatory that you comply with copyright and trademark laws when downloading material from the internet.

If you discover that any damage occurred as a result of downloading software or files, the incident should be reported immediately to your manager and IT.

You may not install other online services to access the internet on company-owned computers, such as America Online, CompuServe, EarthLink, etc. Any questions should be directed to your manager or IT.

6.6 EMAIL

When an email account is assigned to an Employee, any communication sent from that account is the responsibility of the Employee assigned to the account. Employees are prohibited from allowing other individuals to send email from their account and may not use another employee's account to send email communications for their own purposes. Employees should not expect that email communications made through the Companies' system are confidential. Although Employees will be given a username and password, the Companies reserve the right to review the transmissions.

The confidentiality of any message should not be assumed. Even when a message is erased, it is still possible to retrieve and read that message. Further, the use of passwords for security does not guarantee confidentiality. All passwords locking computers or email should be disclosed to the Company. Internal and external email messages are considered business records and may be subject to discovery in the event of litigation. Employees should be aware of this possibility when sending emails within and outside the Company.

The use of email through the Companies' network is primarily for business purposes. Incidental personal use of the email system is permitted. However, the personal use of email should not interfere with company operations, nor should it cause any harm or embarrassment to the Company or their Employees. Any personal use of email is expected to be on the Employees own time and is not to interfere with any job responsibilities.

While on the internet, be careful when giving your email address. The Companies' system may be inundated with "junk" email.

Storage space on the computer is critical. Employees should practice good housekeeping rules including the following:

- Create folders for received and sent messages. Use folders to save important information but make it a regular habit to review all folders and delete old or outdated material. Delete unimportant messages as you read them
- Keep "in" and "sent" boxes clean
- Do not save multiple copies of threads. When sending a message and receiving a response with the original message attached, several layers are created; the last message only needs to be saved
- Do not reply with attachments or use "reply all" unless the response requires it

Proper Email Etiquette

- An email to a client should follow the same formality as a business letter. It should be treated as a formal document with proper business standards being followed. Spelling, grammar, and punctuation should be checked
- Follow the chain of command. Do not copy or jump management levels unless absolutely appropriate
- Use professional language. Never send abusive, harassing, threatening, or unethical messages

- Use common sense about what is said or sent; it is not possible to control who will ultimately read it. Confidentiality and privacy do not exist. A good rule of thumb is “never write anything in an email that you would not want to become public knowledge”
- Review your message before you send it. A sentence that may be clear to someone talking to you face to face might come across quite differently without the tone of your voice or the facial expressions
- Think before sending an email to more than 1 person; respect other Employees’ time. Do the additional people really need or want to see the message? Often an obligation is felt to respond to express opinions
- Always use a short informative subject line. This gives the receiver some indication of the importance of the message
- Be careful when using sarcasm and humour. Without personal interaction, a joke could be viewed as criticism
- Do not type in all caps and keep paragraphs short and concise.
- Set up a signature and use it in every email
- Generally, only focus on 1 subject per message
- Consider using the “@” + name to alert the person that a response may be required

6.7 SOCIAL MEDIA POLICY

This set of rules and guidelines is for any activity and participation in “social media” by all Employees. For purposes of this Handbook, “social media” applies to any web-based and mobile technologies, in use now or developed in the future, that enable individuals or entities to disseminate or receive information, communicate, or otherwise interact, and includes, without limitation, email, texting, messaging, social networking, blogging, micro-blogging, bulletin boards, and so on, through providers such as Facebook, LinkedIn, Myspace, Twitter, YouTube, or Instagram.

These rules and guidelines are intended to be adaptable to the changes in technology and norms of online communication and behaviour and may be amended by the Company at any time, for any reason, without notice to users.

You are personally responsible for any of your social media activity conducted with a company email address or on a company’s website or page, and/or that can be traced back to a company domain, and/or that uses the Companies’ information systems and/or that expressly or implicitly identifies you as an Employee of the Companies.

If from your post in a blog or elsewhere in social media it is clear you are an Employee, or if you mention the Company, or it is reasonably clear you are referring to the Company or a position taken by the Company, and also express a political opinion or an opinion regarding the Companies’ positions and/or actions, the post must specifically note that the opinion expressed is your opinion and not the Companies’ position. This is necessary to preserve the Companies’ good will in the marketplace.

Be sure to state your true identity. When participating in any social media, be completely transparent and disclose your identity for your personal protection. When commenting on or promoting any company product or service on any form of social media, you must clearly and conspicuously disclose your relationship with the Companies to the members and readers of that social media.

Do not use your own personal online relationships or the Companies network to influence polls, rankings, or web traffic. This is called “astroturfing” or “sock-puppeting” and is highly unethical. You are not to use the size and breadth of the Companies’ network to unduly influence polls, rankings, or web traffic where said traffic is a measure of success or popularity of a particular political opinion.

Take special care to observe and follow existing company policy and agreements (such as our Employee Handbook), the policies of the particular online/social networking venue, and applicable law. Do not post any information or conduct any online activity that may violate laws or regulations. Any conduct that under the law is impermissible if expressed in any other form or forum is impermissible if expressed through social media.

You are prohibited from using social media to post or display comments about coworkers or managers or the Company that are vulgar, obscene, threatening, intimidating, or a violation of the Companies' workplace policies against discrimination, harassment, or hostility on account of age, race, religion, sex, gender identity, sexual orientation, ethnicity, nationality, disability, or other protected class, status, or characteristic. Thus, the rules in the Employee Handbook, including its anti-harassment and discrimination policies, apply to Employee behaviour within social media and in public online spaces.

Most websites, including Facebook and others, have rules concerning the use and activity conducted on their sites. These are sometimes referred to a "Terms of Use." You must follow the established terms and conditions of use that have been established by the venue and not violate those rules.

Be respectful and mindful of privacy and confidentiality and think before posting. Before sharing a comment, post, picture, or video about or from a friend or colleague through any type of social media, it is a good practice to be courteous and first obtain your colleague's consent.

It is inappropriate to use and/or disclose personal data information about another individual and use and/or disclose the Companies' confidential or proprietary information in any form of social media. Personal data is information that relates to an identified or identifiable individual. The Companies' confidential or proprietary information includes, but is not limited to, financial information, future business performance and business plans, business and brand strategies, and information that is or relates to the Companies' trade secrets. All company rules regarding the Companies' confidential or proprietary information and personal information, including the Companies' written information security program, apply in full to social media, such as blogs or social networking sites. For example, any information that cannot be disclosed through a conversation, a note, a letter, or an email also cannot be disclosed in a blog. Sharing this type of information, even unintentionally, can potentially result in harm to the individual, harm to the Companies' business, and ultimately the Employee and/or Company being sued by an individual, other businesses or the government.

Before posting any online material, ensure that the material is not knowingly false; instead, try to be accurate and truthful. You should never post anything that is maliciously false. If you find that you've made a mistake, admit it, apologize, correct it, and move on.

Before posting a comment or responding to an online conversation or comment, think before sending. If you are unsure about the effects of the post or other online action, reach out to your manager or HR for some assistance, particularly when unsure about a response to another Employee or a client.

Manage your expectation of privacy. The Company may access and monitor their information systems and obtain the communications within the systems, including email, internet usage, and the like, with or without notice to users of the system, in the ordinary course of business when the Company deems it appropriate to do so. As such, when using such systems, you should have no expectation of privacy with regard to time, frequency, content, or other aspects of your use, including the websites you visit and other internet/intranet activity. The reasons the Company accesses and monitors these systems include, but are not limited to, maintaining the system, preventing, or investigating allegations of system abuse or misuse, assuring compliance with software copyright laws, and complying with legal and regulatory requirements.

It is imperative that you interact on your time. The Company respects the right of any Employee to participate in social media, such as maintaining a blog or participating in online forums. However, to protect the Companies' interests and to ensure Employees focus on their job duties, Employees must avoid excessive use of social media during work time or at any time with the Companies' equipment or property, unless doing so is expressly permitted by the Company.

Avoid personal attacks, online fights, and hostile personalities. If a blogger or any other online influencer posts a statement you disagree with, you can voice your opinion, but do not escalate the conversation to a heated, personal argument. Speak reasonably, factually, and with good humour. Try to understand and credit the other person's point of view. Additionally, avoid communicating with hostile personalities to avoid personal, professional, or credibility attacks.

Identify any copyrighted or borrowed material with citations and links. When publishing any online material through social media that includes another's direct or paraphrased quotes, thoughts, ideas, photos, or videos, always use citations and link to the original material where applicable.

6.8 BYOD (BRING YOUR OWN DEVICE) POLICY

At Bamboo, we recognize the increasing prevalence and importance of personal devices in the workplace. This policy establishes guidelines for employees who are pre-approved to use their personal devices for work-related purposes, promoting productivity, flexibility, and employee satisfaction while ensuring the security and confidentiality of company data.

Scope:

This policy applies to all employees who use personal devices to access, store, or process company data.

Device Eligibility:

- a. With pre-approval certain employees are allowed to use personal devices, such as smartphones, tablets, and laptops, for work-related tasks if they comply with the company's device standards and App requirements
- b. Personal devices must be in good working condition, regularly updated with the latest security patches, and compatible with necessary applications and systems

Security:

- a. Employees must secure their personal devices with strong passwords or biometric authentication and enable automatic lock screens after a period of inactivity
- b. Devices should have up-to-date antivirus software and firewalls installed and enabled
- c. Lost or stolen devices must be reported immediately to the IT department to initiate appropriate security measures, such as remote wiping of company data

Data Protection:

- a. Employees are responsible for ensuring that company data is not shared with unauthorized individuals or stored on unauthorized third-party services or applications
- b. Company data should be stored in designated cloud storage or approved file-sharing platforms with adequate security measures and encryption

c. Personal devices used for work should not be shared with family members, friends, or any other unauthorized individuals

Acceptable Use:

a. Employees must comply with all applicable company policies, including but not limited to the acceptable use of technology resources, data protection, and confidentiality

Support and Maintenance:

a. Employees are responsible for the maintenance and upkeep of their personal devices, including software updates, troubleshooting, and repairs

b. IT support will provide limited assistance related to work-related applications and configurations on personal devices, following established procedures and priorities

Compliance:

a. Employees must comply with all applicable laws, regulations, and industry standards related to the use, storage, and transmission of company data

b. Failure to comply with this policy may result in disciplinary actions, up to and including termination of employment

BAMBOO GDPR COMPLIANCE POLICY

1 PURPOSE

This policy establishes an effective, accountable, and transparent framework for ensuring compliance with the requirements of the GDPR.

2 SCOPE

This policy applies to all Bamboo employees and all third parties responsible for the processing of personal data on behalf of Bamboo.

3 POLICY STATEMENT

Bamboo is committed to conducting its business in accordance with all applicable data protection laws and regulations and in line with the highest standards of ethical conduct.

This policy sets forth the expected conduct of Bamboo employees and third parties in relation to the collection, use, retention, transfer, disclosure and destruction of any personal data belonging to a Bamboo contact (i.e. the data subject).

Personal data is any information (including opinions and intentions) which relates to an identified or identifiable natural person. Personal data is subject to certain legal safeguards and other regulations, which impose restrictions on how organizations may process personal data. An organization that handles personal data and makes decisions about its use is known as a Data Controller. Bamboo, as a Data Controller, is responsible for ensuring compliance with the data protection requirements outlined in this policy. Non-compliance may expose Bamboo to complaints, regulatory action, fines and/or reputational damage. Bamboo, as a Data Processor, is responsible for ensuring compliance with the requirements of the Data Controller and with the data protection requirements outlined in this policy. Non-compliance may expose Bamboo to complaints, regulatory action, fines and/or reputational damage.

Bamboo's leadership is fully committed to ensuring continued and effective implementation of this policy and expects all Bamboo employees and third parties to share in this commitment. Any breach of this policy will be taken seriously and may result in disciplinary action or business sanction.

3.1. GOVERNANCE

Data Protection Officer

To demonstrate our commitment to data protection, and to enhance the effectiveness of our compliance efforts, Bamboo's parent company has appointed a Data Protection Officer. The Data Protection Officer operates with independence and is supported by suitably skilled individuals granted all necessary authority. The Data Protection Officer works with and reports to the Data Privacy Team at Bamboo parent company. The Data Protection Officer's and the Data Privacy Team's duties include:

- Informing and advising Bamboo and its employees who carry out processing pursuant to data protection regulations, national law or European Union based data protection provisions;
- Ensuring the alignment of this policy with applicable data protection regulations, national law or European Union based data protection provisions;
- Providing guidance with regards to carrying out Data Protection Impact Assessments (DPIAs);
- Acting as a point of contact for and cooperating with Data Protection Authorities (DPAs);

- Determining the need for notifications to one or more DPAs because of Bamboo 's current or intended personal data processing activities;
- Making and keeping current notifications to one or more DPAs because of Bamboo 's current or intended personal data processing activities;
- Processing appropriate responses to data subject requests;
- Informing senior managers, officers, and directors of Bamboo of any potential corporate, civil and criminal penalties which may be levied against Bamboo and/or its employees for violation of applicable data protection laws.

Ensuring establishment of procedures and standard contractual provisions for obtaining compliance with this Policy by any third party who:

- Provides personal data to an Bamboo service/entity
- Receives personal data from an Bamboo service/entity
- Has access to personal data collected or processed by Bamboo

Data Protection by Design

To ensure that all data protection requirements are identified and addressed when designing new systems or processes or services and/or when reviewing or expanding existing systems or processes or services, each of them must go through an approval process before continuing. Each Bamboo service/entity must ensure that a Data Protection Impact Assessment (DPIA) is conducted, in cooperation with the Data Protection Officer, for all new and/or revised systems or processes for which it has responsibility. The subsequent findings of the DPIA must then be submitted to the Data Privacy Team for review and approval. Where applicable, any third-party Information Technology (IT) contractors, as part of Bamboo 's IT system and application design review process, will cooperate with the Data Protection Officer to assess the impact of any new technology uses on the security of personal data.

Compliance Monitoring

To confirm that an adequate level of compliance that is being achieved by all Bamboo services/entities in relation to this policy, the Data Protection Officer and Data Privacy Team will carry out an annual data protection compliance audit for all such services/entities. Each audit will, as a minimum, assess:

- Compliance with policy in relation to the protection of personal data, including:
 - The assignment of responsibilities.
 - ✓ Raising awareness.
 - ✓ Training of employees.
- The effectiveness of data protection related operational practices, including:
 - ✓ Data subject rights.
 - ✓ Personal data transfers.
 - ✓ Personal data incident management.
 - ✓ Personal data complaints handling.
 - ✓ The level of understanding of data protection policies and privacy notices.
 - ✓ The currency of data protection policies and privacy notices.
 - ✓ The accuracy of personal data being stored.

- ✓ The conformity of data processor activities.
- ✓ The adequacy of procedures for redressing poor compliance and personal data breaches. The Data Protection Officer, in cooperation with the Data Privacy Team, will devise a plan with a schedule for correcting any identified deficiencies within a defined and reasonable time frame. Any major deficiencies and good practice identified will be reported to, monitored and shared by the Bamboo Data Privacy Team.

3.2. DATA PROTECTION PRINCIPLES

Bamboo has adopted the following principles to govern its collection, use, retention, transfer, disclosure, and destruction of personal data:

Principle 1: Lawfulness, Fairness and Transparency. Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject. This means, Bamboo must tell the data subject what processing will occur (transparency), the processing must match the description given to the data subject (fairness), and it must be for one of the purposes specified in the applicable data protection regulation (lawfulness).

Principle 2: Purpose Limitation. Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. This means Bamboo must specify exactly what the personal data collected will be used for and limit the processing of that personal data to only what is necessary to meet the specified purpose.

Principle 3: Data Minimization. Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. This means Bamboo must not store any personal data beyond what is strictly required.

Principle 4: Accuracy. Personal data should be accurate and, kept up to date. This means Bamboo must have in place processes for identifying and addressing out-of-date, incorrect and redundant personal data.

Principle 5: Storage Limitation. Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. This means Bamboo must, wherever possible, store personal data in a way that limits or prevents identification of the data subject.

Principle 6: Integrity & Confidentiality. Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing, and against accidental loss, destruction or damage. Bamboo must use appropriate technical and organizational measures to ensure the integrity and confidentiality of personal data is maintained at all times.

Principle 7: Accountability. The Data Controller shall be responsible for, and be able to demonstrate, compliance. This means Bamboo must demonstrate that the six data protection principles (outlined above) are met for all personal data for which it is responsible.

3.3. DATA COLLECTION

Data Sources

Personal data should be collected only from the data subject unless one of the following apply:

- The nature of the business purpose necessitates collection of personal data from other persons or bodies.
- The collection must be carried out under emergency circumstances in order to protect the vital interests of the data subject or to prevent serious loss or injury to another person.

If personal data is collected from someone other than the data subject, the data subject must be informed of the collection unless one of the following apply:

- The data subject has received the required information by other means.
- The information must remain confidential due to a professional secrecy obligation
- A national law expressly provides for the collection, processing or transfer of personal data.

Where it has been determined that notification to a data subject is required, notification should occur promptly, but in no case later than:

- One calendar month from the first collection or recording of the personal data
- At the time of first communication if used for communication with the data subject
- At the time of disclosure if disclosed to another recipient.

Data subject consent

Each Bamboo entity will obtain personal data only by lawful and fair means and, where appropriate, with the knowledge and consent of the individual concerned. Where a need exists to request and receive the consent of an individual prior to the collection, use or disclosure of their personal data, Bamboo is committed to seeking such consent. The Data Protection Officer and Data Privacy Team, in cooperation with other relevant business representatives, shall establish a system for obtaining and documenting data subject consent for the collection, processing, and/or transfer of their personal data.

Data subject Notification

Each Bamboo entity will, when required by applicable law or contract, or where it considers that it is reasonably appropriate to do so, provide data subjects with information as to the purpose of the processing of their personal data. When the data subject is asked to give consent to the processing of personal data and when any personal data is collected from the data subject, all appropriate disclosures will be made, in a manner that draws attention to them, unless one of the following apply:

- The data subject already has the information;
- A legal exemption applies to the requirements for disclosure and/or consent. The disclosures may be given orally, electronically or in writing. If given orally, the person making the disclosures should use a suitable script or form approved in advance by the Data Protection Officer. The associated receipt or form should be retained, along with a record of the facts, date, content, and method of disclosure.

External Privacy Notices

Each external website provided by Bamboo will include an online 'Privacy Policy' and an online 'Cookie Policy' fulfilling the requirements of applicable law.

3.4. DATA USE

Data processing

Bamboo uses the personal data of its contacts for the following broad purposes:

- The general running and business administration of Bamboo services/entities.
- To provide services to Bamboo's clients.
- The ongoing administration and management of customer services.

The use of a contact's information should always be considered from their perspective and whether the use will be within their expectations or if they are likely to object. For example, it would clearly be within a contact's expectations that their details will be used by Bamboo to respond to a contact request for information about the products and services. However, it will not be within their reasonable expectations that Bamboo would then provide their details to third parties for marketing purposes.

Each Bamboo service/entity will process personal data in accordance with all applicable laws and applicable contractual obligations. More specifically, Bamboo will not process personal data unless at least one of the following requirements are met:

- The data subject has given **consent** to the processing of their personal data for one or more specific purposes.
- Processing is necessary for the performance of a **contract** to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.
- Processing is necessary for compliance with a **legal obligation** to which the Data Controller is subject.
- Processing is necessary in order to protect the **vital interests** of the data subject or of another natural person.
- Processing is necessary for the performance of a task carried out in the **public interest** or in the exercise of official authority vested in the Data Controller.
- Processing is necessary for the purposes of the **legitimate interests** pursued by the Data Controller/Processor or by a third party (except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject, in particular where the data subject is a child).

There are some circumstances in which personal data may be further processed for purposes that go beyond the original purpose for which the personal data was collected. When making a determination as to the compatibility of the new reason for processing, guidance and approval must be obtained from the Data Protection Officer before any such processing may commence.

- In any circumstance where consent has not been gained for the specific processing in question, Bamboo will address the following additional conditions to determine the fairness and transparency of any processing beyond the original purpose for which the personal data was collected: Any link between the purpose for which the personal data was collected and the reasons for intended further processing.
- The context in which the personal data has been collected, in particular regarding the relationship between the data subject and the Data Controller.
- The nature of the personal data, in particular whether special categories of data are being processed, or whether personal data related to criminal convictions and offences are being processed.
- The possible consequences of the intended further processing for the data subject.
- The existence of appropriate safeguards pertaining to further processing, which may include encryption, anonymisation or pseudonymisation.

Special Categories of Data

Bamboo will only process special categories of data (also known as sensitive data) where the data subject **expressly consents** to such processing or where one of the following conditions apply:

- The processing relates to personal data which has already been made public by the data subject.

- The processing is necessary for the establishment, exercise or defence of legal claims.
- The processing is specifically authorised or required by law.
- The processing is necessary to protect the **vital interests** of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent.
- Further conditions, including limitations, are based upon national law related to the processing of genetic data, biometric data or data concerning health.

In any situation where special categories of data are to be processed, prior approval must be obtained from the Data Protection Officer, and the basis for the processing clearly recorded with the personal data in question. Where special categories of data are being processed, Bamboo will adopt additional protection measures.

Data Quality

Each Bamboo service/entity will adopt all necessary measures to ensure that the personal data it collects, and processes is complete and accurate in the first instance and is updated to reflect the current situation of the data subject. The measures adopted by Bamboo to ensure data quality include:

- Correcting personal data known to be incorrect, inaccurate, incomplete, ambiguous, misleading, or outdated, even if the data subject does not request rectification.
- Keeping personal data only for the period necessary to satisfy the permitted uses or applicable statutory retention period.
- The removal of personal data if in violation of any of the data protection principles or if the personal data is no longer required.
- Restriction, rather than deletion of personal data, insofar as:
 - ✓ a law prohibits erasure.
 - ✓ erasure would impair legitimate interests of the data subject.
 - ✓ the data subject disputes that their personal data is correct, and it cannot be clearly ascertained whether their information is correct or incorrect.

Profiling & Automated Decision Making

Bamboo will only engage in profiling and automated decision-making where it is necessary to enter into, or to perform, a contract with the data subject or where it is authorized by law. Where a Bamboo service/entity utilizes profiling and automated decision-making, this will be disclosed to the relevant data subjects. In such cases the data subject will be given the opportunity to:

- Express their point of view.
- Obtain an explanation for the automated decision.
- Review the logic used by the automated system.
- Supplement the automated system with additional data.
- Have a human carry out a review of the automated decision.
- Contest the automated decision.

Object to the automated decision-making being carried out. Each Bamboo service/entity must also ensure that all profiling and automated decision-making relating to a data subject is based on accurate data.

Digital Marketing

Any Bamboo service/entity wishing to carry out a digital marketing campaign without obtaining prior Consent from the data subject must first have it approved by the Data Privacy Team. Where **personal data** (e.g. case studies

or photographs) processing is approved for digital marketing purposes, the data subject must be informed at the point of first contact that they have the right to object, at any stage, to having their data processed for such purposes. If the data subject puts forward an objection, digital marketing related processing of their personal data must cease immediately, and their details should be kept on **a suppression list** with a record of their opt-out decision, rather than being completely deleted. It should be noted that where digital marketing is carried out in a 'business to business' context, there is no legal requirement to obtain an indication of Consent to carry out digital marketing to individuals provided that they are given the opportunity to opt-out.

Data Retention

To ensure fair processing, personal data will not be retained by Bamboo for longer than necessary in relation to the purposes for which it was originally collected, or for which it was further processed. All personal data should be deleted or destroyed as soon as possible where it has been confirmed that there is no longer a need to retain it.

Data Protection

Each Bamboo service/entity will adopt physical, technical, and organizational measures to ensure the security of personal data. This includes the prevention of loss or damage, unauthorized alteration, access or processing, and other risks to which it may be exposed by virtue of human action or the physical or natural environment. A summary of the personal data related security measures is provided below:

- Prevent unauthorized persons from gaining access to data processing systems in which personal data are processed.
- Prevent people entitled to use a data processing system from accessing personal data beyond their needs and authorisations.
- Ensure that personal data in the course of electronic transmission during transport cannot be read, copied, modified or removed without authorization.
- Ensure that in the case where processing is carried out by a Data Processor, the data can be processed only in accordance with the instructions of the Data Controller.
- Ensure that personal data is protected against undesired destruction or loss.
- Ensure that personal data collected for different purposes can and is processed separately.
- Ensure that personal data is not kept longer than necessary

Data Subject Requests

The Data Protection Officer will establish a system to enable and facilitate the exercise of data subject rights related to:

- Information access.
- Objection to processing.
- Objection to automated decision-making and profiling.
- Restriction of processing.
- Data portability.
- Data rectification.
- Data erasure. If an individual makes a request relating to any of the rights listed above, Bamboo will consider each such request in accordance with all applicable data protection laws and regulations. No administration fee will be charged for considering and/or complying with such a request unless the request is deemed to be unnecessary or excessive in nature.

It should be noted that situations may arise where providing the information requested by a data subject would disclose personal data about another individual. In such cases, information must be redacted or withheld as may be necessary or appropriate to protect that person's rights. Detailed guidance for dealing with requests from data subjects can be found in Bamboo's '**Data Subject Access Rights Policy and Procedure**' document, attached as Attachment A.

Law Enforcement Requests & Disclosures

In certain circumstances, it is permitted that personal data be shared without the knowledge or consent of a data subject. This is the case where the disclosure of the personal data is necessary for any of the following purposes:

- The prevention or detection of crime.
- The apprehension or prosecution of offenders.
- The assessment or collection of a tax or duty.
- By the order of a court or by any rule of law.

If a Bamboo service/entity processes personal data for one of these purposes, then it may apply an exception to the processing rules outlined in this policy but only to the extent that not doing so would be likely to prejudice the case in question. If any Bamboo service/entity receives a request from a court or any regulatory or law enforcement authority for information relating to a Bamboo contact, you must immediately notify the Data Protection Officer and the Data Privacy Team who will provide comprehensive guidance and assistance.

Data Protection Training

All Bamboo employees that have access to personal data will have their responsibilities under this policy outlined to them as part of their staff induction training, and as referenced in employees' applicable Employee Handbooks. In addition, each Bamboo service/entity will receive regular Data Protection training and procedural guidance.

Data Transfers

Bamboo services/entities may transfer personal data to internal or third-party recipients located in another country where that country is recognized as having an adequate level of legal protection for the rights and freedoms of the relevant data subjects. Where transfers need to be made to countries lacking an adequate level of legal protection (i.e. third countries), they must be made in compliance with an approved transfer mechanism. Bamboo services/entities may only transfer personal data where one of the transfer scenarios lists below applies:

- The data subject has given Consent to the proposed transfer.
- The transfer is necessary for the performance of a contract with the data subject
- The transfer is necessary for the implementation of pre-contractual measures taken in response to the data subject's request.
- The transfer is necessary for the conclusion or performance of a contract concluded with a third party in the interest of the data subject.
- The transfer is legally required on important public interest grounds.
- The transfer is necessary for the establishment, exercise or defence of legal claims.
- The transfer is necessary in order to protect the vital interests of the data subject.

Complaint handling

Data subjects with a complaint about the processing of their personal data should put forward the matter in writing to the Data Protection Officer and the Data Privacy Team. An investigation of the complaint will be carried out to the extent that is appropriate based on the merits of the specific case. The Data Protection Officer and the

Data Privacy Team will inform the data subject of the progress and the outcome of the complaint within a reasonable period. If the issue cannot be resolved through consultation between the data subject, the Data Protection Officer, and the Data Privacy Team, then the data subject may, at their option, seek redress through mediation, binding arbitration, litigation, or via complaint to the Data Protection Authority within the applicable jurisdiction.

Breach Reporting

Any individual who suspects that a personal data breach has occurred due to the theft or exposure of personal data must immediately notify the Data Privacy Team and the Data Protection Officer providing a description of what occurred. Notification of the incident can be made to help.us@aptitudehealth.com. The Data Privacy Team and the Data Protection Officer will investigate all reported incidents to confirm whether or not a personal data breach has occurred. If a personal data breach is confirmed, the Data Privacy Team and Data Protection Officer will follow the relevant BAMBOO data breach policy based on the criticality and quantity of the personal data involved.

4 ROLES AND RESPONSIBILITIES

Implementation

The senior management team and senior staff of each Bamboo service/entity must ensure that all Bamboo employees responsible for the processing of personal data are aware of and comply with the contents of this policy. In addition, each Bamboo service/entity will make sure all third parties engaged to process personal data on their behalf (i.e. their data processors) are aware of and comply with the contents of this policy. Assurance of such compliance must be obtained from all third parties, whether companies or individuals, prior to granting them access to personal data controlled by Bamboo.

Support, Advice and Communication

For advice and support in relation to this policy, please contact the Data Privacy Team.

5 REVIEW

This policy will be reviewed by the Data Protection Officer/Data Privacy Team every **three years** unless there are any changes to regulations or legislation that would enable a review earlier.

6 RECORDS MANAGEMENT

Staff must maintain all records relevant to data subject requests or data breaches in electronic form in a recognized Bamboo recordkeeping system.

7 TERMS AND DEFINITIONS

General Data Protection Regulation (GDPR): The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU). It also addresses the export of personal data outside the EU.

Data Controller: the entity that determines the purposes, conditions and means of the processing of personal data.

Data Processor: the entity that processes data on behalf of the Data Controller.

Data Protection Authority: national authorities tasked with the protection of data and privacy as well as monitoring and enforcement of the data protection regulations within the Union.

Data Protection Officer (DPO): an expert on data privacy who works independently to ensure that an entity is adhering to the policies and procedures set forth in the GDPR.

Data subject: a natural person whose personal data is processed by a controller or processor.

Personal data: any information related to a natural person or 'data subject', that can be used to directly or indirectly identify the person.

Privacy Impact Assessment: a tool used to identify and reduce the privacy risks of entities by analysing the personal data that are processed and the policies in place to protect the data.

Processing: any operation performed on personal data, whether or not by automated means, including collection, use, recording, etc.

Profiling: any automated processing of personal data intended to evaluate, analyse, or predict data subject behaviour.

Regulation: a binding legislative act that must be applied in its entirety across the Union.

Subject Access Right: also known as the Right to Access, it entitles the data subject to have access to and information about the personal data that a controller has concerning them.

8 RELATED LEGISLATION AND DOCUMENTS

[Regulation \(EU\) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC \(General Data Protection Regulation\)](#)

ATTACHMENT A

BAMBOO DATA SUBJECT ACCESS REQUEST POLICY AND PROCEDURE

1. PURPOSE

1.1. This policy and procedure establish an effective, accountable, and transparent framework for ensuring compliance with the requirements for Bamboo by the GDPR.

2. SCOPE

2.1. This policy and procedure apply across all entities or subsidiaries owned, controlled, or operated by Bamboo and to all employees, including part-time, temporary, or contract employees, that handle Bamboo data.

3. POLICY STATEMENT

3.1. The GDPR details rights of access to both manual data (which is recorded in a relevant filing system) and electronic data for the data subject. This is known as a Data Subject Access Request (DSAR).

3.2. Under the GDPR, organizations are required to respond to subject access requests within one month. Failure to do so is a breach of the GDPR and could lead to a complaint being made to the Data Protection Regulator.

3.3. This policy informs staff of the process for supplying individuals with the right of access to personal data and the right of access to staff information under the General Data Protection Regulation (hereinafter called GDPR). Specifically:

- All staff need to be aware of their responsibilities to provide information when a data subject access request is received. When a subject access request is received, it should immediately be reported to the Data Protection Officer and the Data Privacy Team to log and track each request.
- Requests must be made in writing (template form is provided, but not mandatory).
- The statutory response time is one month.
- Requests should include the full name, date of birth and address of the person seeking access to their information. To comply with the GDPR, information relating to the individual must only be disclosed to them or someone with their written consent to receive it.
- No fee can be charged for initial DSAR for all types of records, whether manual or electronic format.

4. PROCEDURE

How should DSARs be processed after receiving them?

When a subject access request is received from a data subject it should immediately be reported to the Data Protection Officer and the Data Privacy Team, who will log and track each request. If you are asked to provide information, you will need to consider the following before deciding how to respond:

- Under GDPR Articles 7(3), 12, 13, 15-22 data subjects have the following rights:
 - to be informed;
 - to access their own data;
 - to rectification;
 - to erasure (Right to be Forgotten);
 - to restriction of processing;

- to be notified;
 - to data portability;
 - to object;
 - to object to automated decision making.
- Requests must be made in writing (template form is attached but is not mandatory). All DSARs received by email, mail, fax, social media, etc. must be processed.
 - The type of access you must provide and the fee you are allowed to charge may vary depending on how the records are held. It does not have to state 'subject access request' or 'data protection' to constitute a request under the GDPR.
 - If a request has already been complied with and an identical or similar request is received from the same individual a fee can be charged for the second request unless a reasonable interval has elapsed.
 - The statutory response time is one month.
 - Requests should include the full name, date of birth and address of the person seeking access to their information. To comply with the GDPR, information relating to the individual must only be disclosed to them or someone with their written consent to receive it.
 - Before processing a request, the requestor's identity must be verified. Examples of suitable documentation include:
 - Valid Passport
 - Valid Identity Card
 - Valid Driver's License
 - Birth Certificate along with some other proof of address e.g. a named utility bill (no longer than 3 months old)

Fees

4.1. No fee can be charged for providing information in response to a data subject access request, unless the request is 'manifestly unfounded or excessive', in particular because it is repetitive.

If Bamboo receives a request that is manifestly unfounded or excessive, it will charge a reasonable fee taking into account the administrative costs of responding to the request. Alternatively, Bamboo will be able to refuse to act on the request.

Subject access requests made by a representative or third party

4.2. Anyone with full mental capacity can authorize a representative/third party to help them make a data subject access request. Before disclosing any information, Bamboo must be satisfied that the third party has the authority to make the request on behalf of the requestor and that the appropriate authorization to act on their behalf is included.

Complaints

4.3. If an individual is dissatisfied with the way Bamboo has dealt with their subject access request, they should be advised to invoke the Bamboo complaints process. If they are still dissatisfied, they can complain to the Data Protection Regulator.

5. RESPONSIBILITIES

Compliance, monitoring and review

5.1. The overall responsibility for ensuring compliance with the requirements of the related legislation in relation to performing subject access rights at Bamboo rests with the Data Protection Officer and the Data Privacy Team.

5.2. All operating units' staff that deal with personal data are responsible for processing this data in full compliance with the relevant Bamboo policies and procedures.

Records management

5.3. Staff must maintain all records relevant to administering this policy and procedure in electronic form in a recognized Bamboo recordkeeping system.

6. TERMS AND DEFINITIONS

General Data Protection Regulation (GDPR): the General Data Protection Regulation (GDPR) (Regulation(EU) 2016/679) is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU). It also addresses the export of personal data outside the EU.

Data Controller: the entity that determines the purposes, conditions and means of the processing of personal data

Data Processor: the entity that processes data on behalf of the Data Controller

Data Protection Authority: national authorities tasked with the protection of data and privacy as well as monitoring and enforcement of the data protection regulations within the European Union

Data Protection Officer (DPO): an expert on data privacy who works independently to ensure that an entity is adhering to the policies and procedures set forth in the GDPR

Data Subject: a natural person whose personal data is processed by a controller or processor

DSAR: data subject access request

Personal Data: any information related to a natural person or 'Data Subject', that can be used to directly or indirectly identify the person

Privacy Impact Assessment: a tool used to identify and reduce the privacy risks of entities by analysing the personal data that are processed and the policies in place to protect the data

Processing: any operation performed on personal data, whether or not by automated means, including collection, use, recording, etc.

Profiling: any automated processing of personal data intended to evaluate, analyse, or predict data subject behaviour

Regulation: a binding legislative act that must be applied in its entirety across the European Union

Subject Access Right: also known as the Right to Access, it entitles the data subject to have access to and information about the personal data that a controller has concerning them.

7. RELATED LEGISLATION AND DOCUMENTS

[Regulation \(EU\) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC \(General Data Protection Regulation\)](#)

7 ACKNOWLEDGEMENTS

7.1 RECEIPT AND ACKNOWLEDGEMENT OF HANDBOOK

I acknowledge receipt of the Bamboo Employee Handbook. I understand that the Handbook is not contractual in nature and does not create an express nor implied contract of employment with the Company. By signing this Receipt and Acknowledgement, I acknowledge that I have read this Handbook and am familiar with its policies, including the Equal Employment and Anti-Harassment policies. I understand that, should I have any questions about **any** of the policies contained herein, I should address any questions with my manager or with the Human Resources department.


I further understand that no representative of the Company, other than the CEO (or any individual specifically authorized by the CEO), is authorized to modify this Handbook or to enter into any agreement or contract containing provisions contrary to those described in this Handbook. This Handbook shall not be modified by any statements contained in any Employee manuals, personnel policies manual, employment applications, the Companies' recruiting materials, offers of employment, the Companies' memorandums, or other materials provided to Employees in connection with their employment.

I further understand that this Handbook supersedes all previous handbooks or policies that I may have been given.

I HAVE READ THE ABOVE STATEMENTS AND UNDERSTAND THE EMPLOYEE HANDBOOK.

James Lalor

Printed Employee Name

DocuSigned by:

F5CDBEBF4BEB4AA...

3/6/2024

Employee Signature

Date