Title:	**Email & Electronic Messaging Policy**
Code:	**WBEEM-01**
Published:	**July 2023**
Review date:	**July 2024**
Approved by:	**SMT**
Policy owner:	**Chief Financial Officer (CFO)**

Table of contents

WaterBear is a College of Falmouth University and as such its students are students of Falmouth University, studying at WaterBear. All WaterBear policies and procedures have been tailored to best suit the specific requirements of the College, its students and staff. In some instances, Falmouth policies and procedures may be deferred to for additional guidance, or where Falmouth policy has been deemed to cover both the requirements of the University's operations and those of its academic partners.

This policy applies to any student, prospective student and applicant of WaterBear in receipt of a direct service from the College.

Purpose

The purpose of this policy is to ensure that WaterBear Users use the electronic and emailing system properly and that no breach of any personal data occurs.

This policy applies to all Users that use the emailing and electronic messaging system (referred to as the Email System).

In this policy, the terms "messages" and "emails" are used interchangeably and do not exclude each other. Both terms refer to electronic communications and should be understood to encompass the broad spectrum of electronic communications without any distinction or preference between the two terms.

Privacy and Conditions of Accessing Email [ending in the suffix @waterbear.org.uk]

Under the conditions of this policy, no User should monitor another User's email account. The monitoring and inspection of the Email System should be done only by authorised people, when necessary, to avoid any violation of the policy. The right to retrieve data is used with the intention of monitoring data in any case of system failure, lost messages, or emails. In this way, WaterBear would be able to comply with the legal obligations in place.

To the extent permitted or required by law, the Company may monitor Users' use of the Company's electronic messaging for its legitimate business purposes which include (but are not necessarily limited to) the following reasons:

- To ensure Company policies and guidelines are followed, and standards of service are maintained;
- To comply with any legal obligation;
- To investigate and prevent the unauthorised use of the Company's Email System and maintain security;
- If the Company suspects that a User has been viewing or sending offensive or illegal material (or material that is otherwise in violation of this Policy);
- If the Company suspects that a User has been spending an excessive amount of time using the Company's Email System for personal purposes.

Security of the Email System

WaterBear has installed different antivirus software to ensure the protection of employee and student personal data and prevention and removal of unwanted emails. These programs do not guarantee that no breach of personal information will occur; however, they do ensure a level of safety while

using the Email System. In case there is any suspicious or offensive email received or sent by Users, such acts should immediately be reported to the persons responsible in the IT department and the top management.

WaterBear has created a system which provides access to encryption methods for all users, hence complying with the GDPR encryption regulation.

When opening emails from external sources Users must exercise caution considering items such as malware, spyware, viruses, and other malicious software or code that poses a risk to system security. Users should always ensure that they know what an attachment is before opening it. If a User suspects that their computer has been affected by a virus, they must contact the CEO/CFO immediately.

Appropriate use of the Email System

WaterBear provides email and electronic messaging system for all Users to facilitate the communication among them and external interested parties. Such systems are intended to be used for work-related purposes, however Users may use Company email for personal purposes, provided that such use is kept to a minimum and does not interfere with the performance of the User's duties. Users are reminded that any permitted personal emails should be marked as "personal" in the subject line.

The messages and emails should be written in accordance with the WaterBear practices, and no breach or misinterpretation of any personal information is tolerated as per the GDPR regulation.

Users must not email any business document to their own or a colleague's personal web-based email accounts.

Users are permitted to access and use their personal email accounts only to the extent that such use is reasonable and does not interfere with the User's performance of their duties.

Misuse of the Email System

The misuse of the Email System by transmission of any confidential information of any personal data will be considered as a breach of this policy.

Users should not:

- Send a message which may breach this policy
- Send a message which may contain discriminatory content in regard to sex, gender, religion, philosophical beliefs, etc.
- Send a message containing malicious information

- Send an unencrypted email which contains personally identifiable information of the data subject as per the GDPR regulations
- Send messages from any other User's account
- Forward any personal confidential information of an employee or student without prior approval

Any User found to be misusing the Company's Email System will be treated in line with the Company's Disciplinary Policy and Procedure. Misuse can, in some cases, result in a breach of the General Data Protection Regulation (GDPR), Data Protection Act 2018, Computer Misuse Act 1990.

Where any evidence of misuse of the Company's Email System is found, the Company may undertake an investigation into the misuse in accordance with the Company's Disciplinary Policy and Procedure. If criminal activity is suspected, the Company may hand over relevant information to the police in connection with a criminal investigation.

Receiving Misdirected or Unsuitable Emails

In any case when any of the WaterBear Users receive a misdirected email containing confidential information, the receiver should immediately inform the sender and not disclose or use that certain information. In case the receiver of the email receives information that somehow contains offensive or inappropriate information, the email should be directed to the top management for further investigation.

Sending Personal Data via Email

All personally identifiable data of the WaterBear Users including reports, or any other documentation type should be sent through an encrypted email, and password of the encrypted files should always be sent in a separate email.