COMMUNICATIONS POLICY

This policy applies to your employment at *[Insert Organisation address]* and all other Organisation sites that you may be asked to work at from time to time. This policy must also be observed when visiting and using client or partner facilities. Employees must also comply fully with whatever policy or guidelines exist at client or partner sites.

Please note that this policy also applies to you if you are working as a contractor, agency worker, temporary worker or volunteer within the Organisation.

For any policy to be effective it must be applied throughout the Organisation and apply to all staff regardless of position or seniority.

If you have any questions regarding these guidelines and how they apply to you please consult *[Insert manager's name], [Insert manager's position]* before taking any action that may breach this policy.

This policy does not form part of your contract of employment.

1. Minor Breaches
Minor breaches of this policy shall constitute a disciplinary offence and will be dealt with using the disciplinary procedures of the Organisation.

2. Major Breaches
Major or serious breaches of this policy shall constitute gross misconduct and shall allow the Organisation to terminate your employment, immediately, without notice. Or terminate your contract immediately without notice if you are a contractor, agency or temporary worker.

3. Monitoring

3.1 The Organisation reserves the right to monitor all external and internal communications and access to the Organisation network, intranet and the Internet, (as applicable) where the property of the Organisation is used in the communication or is accessed remotely from outside the Organisation. This includes the use of portable computers and mobile devices, including mobile phones issued to the employee by the Organisation.

3.2 The Organisation reserves the right to use the following methods for monitoring of communications:

Server log file analysis.
Data packet analysis.
Email message analysis, including content of individual emails and attachments where required.
Telephone number analysis.

3.3 In accordance with the General Data Protection Regulation (GDPR) the Organisation will carry out Data Protection Impact Assessments (DPIAs) to assess the impact of any monitoring or extension to existing monitoring within the Organisation prior to its introduction. Any assessment will consider the following:

3.3.1 The reason for implementing or extending monitoring and whether it is justified.

3.3.2 The likely adverse impact on employees and third parties communicating with the Organisation.

3.3.3 The use of alternatives to monitoring or alternative methods of monitoring.

3.3.4 Any additional obligations that arise due to the monitoring, for example the secure storage of and access to information gathered by monitoring.

3.4 The Organisation will also consider the impact of monitoring on employees such as:

3.4.1 The risk of intrusion into employees' private lives.

3.4.2 The extent to which employees will be aware of the monitoring.

3.4.3 The impact monitoring will have on the relationship between employees and the Organisation.

3.4.4 How monitoring will be perceived by employees.

3.5 The Organisation shall inform all workers prior to the introduction of any such monitoring or the extension of any existing monitoring. Furthermore, the Organisation will inform individual workers if their communications are being specifically monitored or accessed. However, an individual will not be informed where serious breaches of the policy or criminal activity is suspected and where informing the individual would hamper any investigation or risk the loss of data and evidence.

3.6 The Organisation shall take all reasonable steps to ensure that personal communications are not accessed during monitoring. However, the Organisation can access personal communications where such communication is partly used to pass information belonging to the Organisation or where the nature of the personal communication provides evidence of the breach of this communications policy.

3.7 The Organisation shall not be liable for any breach of privacy should any communications of a personal nature be found and accessed by employees of the Organisation or third parties authorised by the Organisation and acting in the course of their employment.

4. Usernames and Passwords

4.1 You have a duty to keep safe all usernames and or passwords required to access your PC, portable computer or any other mobile device that you are authorised to use by the Organisation.

4.2 For reasons of security you should not leave usernames and or passwords attached to or near your PC, portable computer or mobile device. If your usernames and or passwords are left on or in your desk, workstation, briefcase, carry case or any personal item they should not be readily identifiable as such.

4.3 You should immediately comply with any request from *[Insert manager's name]* to change your usernames and or passwords.

4.4 Where possible and whenever requested usernames and or passwords should be made up of a combination of letters and numbers and should not consist of names or regular words that may be guessed by a fellow employee, a third party or by software tools specifically designed to ascertain usernames and or passwords.

4.5 If you have any reason to believe that your usernames and or passwords have become known to another party including a fellow employee who is not authorised to have access to your usernames and or passwords you must inform *[Insert manager's name]* immediately and if known provide details of how your usernames and or passwords became known to that party.

5. Internet Usage

6. Social Networking Sites & Data

7. Personal Social Media

8. Password Protected Areas

9. Email Usage Guidelines

10. Emails are Permanent

11. Proper Deletion of Emails

12. Email Signature File

13. Email Etiquette

14. Third Party Products, Software & Apps

15. Downloads and Attachments

16. Transportation and Security

17. Organisation Access

18. Telephone Use

19. Mobile Phone Use

20. Authority

21. Date of Implementation

22. Questions

23. Alteration of this Policy