# Acceptable IT and Communications use policy

1. Overview
   * 1. The Company seeks to provide its employees and visitors with secure and timely access to IT and communications equipment, and the online services and resources necessary for undertaking their work.
     2. The purpose of this policy is to: give a clear statement to all users of The Company’s IT and communication facilities and services of their responsibilities, including what constitutes acceptable and unacceptable use; and manage the provision and modification of access to online services
2. Application

This policy applies to all:

* + 1. permanent employees (including full time and part time);
    2. fixed-term employees;
    3. casual employees; and
    4. temporary agency staff and contractors.

1. Email
   * 1. All email is the property of The Company and may be monitored and audited by appropriately authorised The Company personnel.
     2. All existing Company policies apply to email usage, particularly (but not exclusively) those that relate to Code of Conduct, intellectual property protection, privacy, misuse of company resources, harassment, discrimination, bullying and victimisation, information and data security and confidentiality.
     3. Email content must not be detrimental to, nor adversely affect, the reputation and operations of The Company, its employees, clients or customers. Employees are responsible, and accountable, for their use of email and for the format and content of messages sent by them.
     4. At times, employees may receive emails which they have not solicited or encouraged and which breach The Company email standards. In these instances, such emails must not be forwarded, but deleted, and reasonable steps to prevent a reoccurrence should be taken.
2. Internet
   * 1. As a business tool, the internet represents a considerable commitment of telecommunications, networking, software and storage facilities. It therefore needs to be used primarily for business purposes.
     2. Unnecessary or unauthorised internet usage can severely compromise The Company, so The Company reserves the right to monitor and record internet usage and web browsing activity of all of its employees whilst at work.
     3. All existing The Company policies apply to internet usage, particularly (but not exclusively) those that relate to Code of Conduct, intellectual property protection, privacy, misuse of company resources, harassment, discrimination, bullying and victimisation, information and data security and confidentiality.
     4. Internet activity must not be detrimental to, nor adversely affect, the reputation and operations of The Company, its employees, clients or customers.
3. Prohibited email, internet or communications activity
   * 1. Employees must not use, and must not allow others to use, The Company’s internet or communication services for any of the following:
        1. harassment of any group or individual;
        2. accessing, downloading or distributing any pornographic or other offensive material;
        3. trafficking in confidential customer or client information;
        4. broadcasting e-mails of a defamatory nature;
        5. hacking or entering into any email communications that may be deemed unlawful;
        6. propagation of unsolicited bulk email (also known as spam);
        7. distribution of material that is defamatory, abusive, menacing, threatening, harassing or illegal under legislation where transmissions are sent from, viewed or received;
        8. transmission of unsolicited mail, advertising material or any other material which is offensive or indecent or otherwise contrary to law or relevant The Company policies;
        9. unauthorised copy or distribution of material such as copyrighted works or confidential information;
        10. commission of a crime, activity in the course of commission of a crime or for unlawful purpose;
        11. activities carried out in a manner which could expose The Company, or any entity with which it conducts business, to loss or liability;
        12. actions that may damage the network or systems or cause impairment of their quality and integrity; or
        13. activity that does not comply with The Company's operating procedures, policies and behavioural standards.
     2. Any employee found to have breached this policy in any way will be subject to disciplinary action. The disciplinary action may include termination of employment.
4. Further information

If you require additional information, please speak with your manager.