Systems Usage Policy

About this policy

Our IT and communications systems are intended to promote effective communication and working practices within our organisation. The purpose of this policy is to outline the standards you must observe when using these systems, the circumstances in which we will monitor your use, and the action we will take in respect of breaches of these standards.

This policy does not form part of any contract of employment or other contract to provide services, and we may amend it at any time.

Misuse of IT and communications systems can damage the business and our reputation, lead to unauthorised access to the data we hold. Breach of this policy may be dealt with under our Disciplinary Procedure and, in serious cases, may be treated as gross misconduct leading to summary dismissal.

Who does this policy apply to?

This policy applies to all employees, officers, consultants, self-employed contractors, casual workers, agency workers, volunteers and interns of Briggs Equipment Ireland Limited and all of its direct and indirect subsidiaries. It also applies to anyone who has access to our IT and communication systems.

Who is responsible for this policy?

The board of directors (the Board) has overall responsibility for the effective operation of this policy. The Board has delegated responsibility for overseeing its implementation to the Group Head of the IT Department. Suggestions for changes to this policy should be reported to the Group Head of the IT Department.

Any questions you may have about the day-to-day application of this policy should be referred to your line manager or the IT Department in the first instance. The IT Department provides IT support (including dealing with any requests for permission or assistance under this policy) and may specify certain standards of equipment or procedures to ensure security and compatibility.

This policy is reviewed annually by the IT Department.

Use of own devices and systems

Where required to perform your duties, the Company will provide you with appropriate hardware (laptops, mobile phones etc.) and software (e.g. MS 365, ERP Software etc.).

You must not use any non-Company provided hardware or devices (such as personally owned laptops, tablets or smartphones) or personally registered software (such as webmail accounts, google drive, icloud etc.) in the performance of your duties.

Equipment security and passwords

You are responsible for the security of the equipment allocated to or used by you, and must not allow it to be used by anyone other than in accordance with this policy.

You are responsible for the security of any computer terminal used by you. You should lock your terminal or log off when leaving it unattended or on leaving the office, to prevent unauthorised users accessing the system in your absence. Anyone who is not authorised to access our network should only be allowed to use terminals under supervision.

Desktop PCs and cabling for telephones or computer equipment should not be moved or tampered with without first consulting the IT Department.

You should use passwords and multifactor authentication where applicable on all IT equipment and software, particularly items that you take out of the office. You must keep your passwords confidential and change them regularly. You must not use another person's username and password or make available or allow anyone else to log on using your username and password unless authorised by the IT Department. On the termination of employment (for any reason) you must provide details of your passwords to the IT Department and return any equipment, YubiKeys, access key fobs or cards.

If you have been issued with a laptop, tablet computer, smartphone or other mobile device, you must ensure that it is kept secure at all times, especially when travelling. Passwords must be used to secure access to data kept on such equipment to ensure that confidential data is protected in the event of loss or theft. You should also be aware that when using equipment away from the workplace, documents may be read by third parties, for example, passengers on public transport.

Systems and data security

You should not delete, destroy or modify existing systems, programs, information or data (except as authorised in the proper performance of your duties).

You must not download or install software from external sources without authorisation from the IT Department. This includes software programs, instant messaging programs, screensavers, photos, video clips and music files. Incoming files and data should always be virus-checked by the IT Department before they are downloaded. If in doubt, staff should seek advice from the IT Department.

You must not attach any device or equipment to our systems without authorisation from the IT Department. This includes any USB storage device , Music or video player, tablet, smartphone or other similar device, whether connected via the USB port, Blue-Tooth connection or in any other way.

We monitor all emails passing through our system for viruses. You should exercise particular caution when opening unsolicited emails from unknown sources or an email which appears suspicious (for example, if it contains a file whose name ends in .exe). Inform the IT Department immediately if you suspect your computer may have a virus.

We reserve the right to delete or block access to emails or attachments in the interests of security. We also reserve the right not to transmit any email message.

You should not attempt to gain access to restricted areas of the network, or to any password-protected information, except as authorised in the proper performance of your duties.

You must be particularly vigilant if you use our IT equipment outside the workplace and take such precautions as we may require from time to time against importing viruses or compromising system security. The system contains information which is confidential and subject to data protection legislation. Such information must be treated with extreme care and in accordance with our Data Protection Policy.

Email

Although email is a vital business tool, you should always consider if it is the appropriate method for a particular communication. Correspondence with third parties by email should be written as professionally as a letter.

Messages should be concise and directed only to relevant individuals. Our standard disclaimer should always be included.

You should access your emails at least once every working day, stay in touch by remote access when travelling in connection with business, and use an out of office response when away from the office for more than a day. You should endeavour to respond to emails marked "high priority" within 24 hours.

You must not send abusive, obscene, discriminatory, racist, harassing, derogatory, defamatory, pornographic or otherwise inappropriate emails. Anyone who feels that they are being or have been harassed or bullied, or is offended by material received from a colleague via email, should inform the HR Department.

You should take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract. Remember that you have no control over where your email may be forwarded by the recipient. Avoid saying anything which would cause offence or embarrassment if it was forwarded to colleagues or third parties, or found its way into the public domain.

Email messages are required to be disclosed in legal proceedings in the same way as paper documents. Deletion from a user's inbox or archives does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable, either from the main server or using specialist software.

In general, you should not:

- Send, forward or read private emails at work which you would not want a third party to read.
- Send or forward chain mail, junk mail, cartoons, jokes or gossip.
- Contribute to system congestion by sending trivial messages, copying or forwarding emails to those who do not have a real need to receive them, or using "reply all" unnecessarily on an email with a large distribution list.
- Sell or advertise using our communication systems or broadcast messages about lost property, sponsorship.
- Agree to terms, enter into contractual commitments or make representations by email unless appropriate authority has been obtained. A name typed at the end of an email is a signature in the same way as a name written at the end of a letter.
- Download or email text, music or any other content on the internet which is subject to copyright protection, unless it is clear that the owner of such works allows this.
- Send messages from another person's email address (unless authorised) or under an assumed name.
- Send confidential messages via email or the internet, or by other means of external communication which are known not to be secure.

If you receive an email in error, you should inform the sender.

Do not use your own personal email account to send or receive email for the purposes of our business. Only use the email account we have provided for you.

Using the internet

Internet access is provided solely for business purposes. Occasional personal use may be permitted as set out below.

When a website is visited, devices such as cookies, tags or web beacons may be employed to enable the site owner to identify and monitor visitors. If the website is of a kind described below, such a marker could be a source of embarrassment to the visitor and us, especially if inappropriate material has been accessed, downloaded, stored or forwarded from the website. Such actions may also, in certain circumstances, amount to a criminal offence if, for example, the material is pornographic in nature. This is further considered below.

You should not access any web page or download any image, document or other file from the internet which could be regarded as illegal, offensive, discriminatory, in bad taste or immoral. Even web content which is legal in the UK may be in sufficient bad taste to fall within this prohibition. As a general rule, if any person (whether intended to view the page or not) might be offended by the contents of a page, or if the fact that our software has accessed the page or file might be a source of embarrassment if made public, then viewing it will be a breach of this policy.

Except as authorised in the proper performance of your duties, you should not under any circumstances use our systems to participate in any internet chat room, post messages on any internet message board or set up or log text or information on a blog or wiki, even in your own time.

The following must never be accessed from our network or using a device you have been issued with by us: online radio, audio and video streaming (including streaming of, or downloading of, television radio or films), instant messaging, webmail (such as Gmail or Hotmail) and social networking sites (including, but not limited to, Facebook, Twitter, YouTube, Google+, Instagram, SnapChat, Pinterest, Tumblr, Second Life). This list may be modified from time to time.

Personal use of our systems

We permit the incidental use of our internet, email and telephone systems to send personal email, browse the internet and make personal telephone calls subject to certain conditions set out below. Personal use is a privilege and not a right. It must not be overused or abused. We may withdraw permission for it at any time or restrict access at our discretion.

Personal use must meet the following conditions:

- Use must be minimal and take place substantially out of normal working hours (that is, during lunch hours, before 9.00 am or after 5.30 pm).
- Personal emails should be labelled "personal" in the subject header.
- Use must not interfere with business or office commitments.
- Use must not commit us to any marginal costs.
- Use must comply with this policy and our other policies including the Diversity, Equity and Inclusion Policy, Anti-harassment and Bullying Policy, Data Protection Policy, Disciplinary Rules and Disciplinary Procedure.

You should be aware that personal use of our systems may be monitored (see below) and, where breaches of this policy are found, action may be taken under the disciplinary procedure (see below). We reserve the right to restrict or prevent access to certain telephone numbers or internet sites if we consider personal use to be excessive.

Bring Your Own Device (BYOD)

We do not operate a BYOD policy. Use of personal devices for work purposes is not permitted.

Monitoring

Our systems enable us to monitor telephone, email, voicemail, internet and other communications. For business reasons, and in order to carry out legal obligations in our role as an employer, use of our systems including the telephone and computer systems, and any personal use of them, may be continually monitored by automated software or otherwise. Monitoring is only carried out to the extent permitted or as required by law and as necessary and justifiable for business purposes.

CCTV systems monitor the exterior of the buildings on our sites and high risk area's 24 hours a day. This data is recorded for a limited time.

We reserve the right to retrieve the contents of email messages or to check internet usage (including pages visited and searches made) as reasonably necessary in the interests of the business, including for the following purposes (this list is not exhaustive):

- To monitor whether use of the email system or the internet is legitimate and in accordance with this policy.
- To find lost messages or to retrieve messages lost due to computer failure.
- To assist in the investigation of alleged wrongdoing.
- To comply with any legal obligation.

Prohibited use of our systems

Misuse or excessive personal use of our telephone or email system or inappropriate internet use will be dealt with under our Disciplinary Procedure. Misuse of the internet can in some circumstances be a criminal offence. In particular, it will usually amount to gross misconduct to misuse our systems by participating in online gambling, forwarding chain letters, or by creating, viewing, accessing, transmitting or downloading any of the following material (this list is not exhaustive):

- Pornographic material (that is, writing, pictures, films and video clips of a sexually explicit or arousing nature).
- Offensive, obscene, or criminal material or material which is liable to cause embarrassment to us or to our clients or customers.
- A false and defamatory statement about any person or organisation.
- Material which is discriminatory, offensive, derogatory or may cause embarrassment to others (including material which breaches our Diversity, Equity and Inclusion Policy or our Anti-harassment and Bullying Policy).
- Confidential information about us, our business, or any of our staff, clients or customers (except as authorised in the proper performance of your duties).

Unauthorised software.

Any other statement which is likely to create any criminal or civil liability (for you or us). Music or video files or other material in breach of copyright.

Any such action will be treated very seriously and is likely to result in summary dismissal.

Where evidence of misuse is found, we may undertake a more detailed investigation in accordance with our Disciplinary Procedure, involving the examination and disclosure of monitoring records to those nominated to undertake the investigation and any witnesses or managers involved in the Disciplinary Procedure. If necessary, such information may be handed to the police in connection with a criminal investigation.