Auxo Group Acceptable Use Policy

This document is approved and authorised for application within Auxo Group and all associated subsidiary companies.

Ford Garrard, CEO

Last Review Date: October 2024

Contents

Purpose of the policy

This policy sets out the Auxo Group policy for use of its facilities and networking sites and covers all individuals working at all levels and grades, including senior managers, officers, directors, employees, consultants, contractors, trainees, home workers, part-time and fixed-term employees, casual and agency staff, temporary workers, and volunteers. 'You', 'your' and 'yourself' shall be construed accordingly and where there are references to "employee" and/or "your employment" throughout this document, these should be read as referring to the terms upon which you are either employed or engaged by the Auxo Group (as applicable). Third parties with access to our electronic communication systems and equipment must also comply with this policy. This policy shall apply during the course of your employment including any period of garden leave (and where stated, also after your employment has ended).

The IT department assigns IT devices to users, proportionate to their role and function within the firm. AUXOIT devices are defined as desktop, laptop, tablet or netbook computers, printers, copiers, monitors, servers, handheld devices, telephones, mobile phones, disc drives or any storage device, network switches, routers, wireless access points, batteries, backup tapes, etc.

Definitions

"Confidential Information" means:

- Information relating to the Auxo Group business plans, finances, new or maturing business opportunities, and research and development projects
- Marketing information relating to marketing or sales of any past, present or future service including without limitation sales targets and statistics, market share and pricing statistics, marketing surveys and plans, market research reports, sales techniques and price lists
- Details of professional contacts including names, addresses, contact details, terms of business or proposed terms of business with them, their business requirements, pricing structures, lists of employees and their terms of employment
- Any other information of a confidential nature belonging to employees, candidates, clients, and employees of clients of the Auxo Group or in respect of which the Auxo Group owes any other obligation of confidence

"Data Protection Laws" means the Data Protection Act 2018, the General Data Protection Regulation as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 and any applicable statutory or regulatory provisions in force from time to time relating to the protection and transfer of personal data.

"Facilities" means telephone and computer facilities, including email and the internet, and hardware including mobile media such as laptops, mobile phones, smartphones, personal digital assistants, tablets, notebooks, or similar equipment.

"Jobs Boards" includes sites where candidates and prospective candidates indicate their interest in looking for new job opportunities, and where clients and prospective clients indicate they have vacancies or are looking for new staff. Your access to and use of jobs boards, whilst employed by the company is set out in this policy.

"Networking Sites" includes (but is not limited to) professional networking sites such as LinkedIn, Xing, Viadeo (professional networking sites) and social networking sites such as Facebook, Twitter, Instagram (social networking sites). Your access to and use of networking sites, whilst employed by the Auxo Group is set out in this policy.

"Personal Contacts" means any of your friends (not including professional contacts).

"Personal Data Request" means any request an individual is entitled to make to the Auxo Group under the Data Protection Laws.

"Professional Contacts" means any candidate, client, introducer, key employee, prospective candidate or prospective client (all as defined in the Annex), together with any contacts made through a professional body trade or association of which you or the Auxo Group is a member.

Use of the facilities

Work use of the Facilities

The facilities are available to you during your employment with the Auxo Group to help you carry out and promote the Auxo Group's business and interests.

Personal use of the facilities

The facilities may be used within reason, for personal communications or to send and retrieve personal messages and to browse external websites for personal use although this should be done outside office hours and be kept to a reasonable limit. It must not interfere with business commitments. If there is evidence that this privilege is being abused, it may be withdrawn. The content of personal e-mails must also comply with the restrictions set out in in the 'Prohibited use of the Facilities' section of this policy. If using the facilities for personal communications, you should be aware that the Auxo Group may monitor your use of the facilities in accordance with the 'Monitoring use of the Facilities, Professional and Social Networking Sites' section of this policy and any breaches of this policy may result in disciplinary action up to and including dismissal.

Prohibited use of the facilities

The following uses of the facilities are expressly prohibited:

- Viewing internet sites which contain pornographic, obscene, abusive, slanderous or otherwise offensive material or downloading or forwarding such material within or outside the Auxo Group
- Sending, receiving or forwarding communications that are in violation of company policy including, but not limited to, the transmission of obscene, offensive or harassing messages
- Sending, receiving or forwarding communications which make unsubstantiated and potentially defamatory comments about colleagues, clients, candidates or any other person via the facilities or any networking site. You are reminded that communications via social media constitutes publication just as printing in hard copy or via email is publication. You personally, and/or the Auxo Group could face a defamation action should you publish unsubstantiated and potentially defamatory material
- Bullying or harassing colleagues, clients, candidates or any other person via the facilities or any networking sites
- Discriminating or making offensive or derogatory comments about any colleagues, clients, candidates or any other person via the facilities or any networking site
- Breaching any other company policies including, but not limited to, the Data Protection Policy, Data Protection Procedure and the Equal Opportunities and Diversity Policy
- Engaging in any behaviour which might cause either the Auxo Group to be in breach of the REC Code of Professional Conduct or you to be in breach of the Institute of Recruitment Professionals Code of Ethics (if you are a member of that institute)
- Duplicating copyrighted or licensed software or other information without the appropriate authorisation
- Installing or downloading any software or hardware without the specific approval of the Auxo Group IT department or other person delegated by them to give such approval

- Forwarding or otherwise perpetuating junk mail or 'chain-letter' type e-mail within or outside the Auxo Group
- Removing any hardware or software from the facilities or the Auxo Group premises without prior approval of the Auxo Group IT department
- Selling or advertising anything via the facilities or broadcast messages about lost property, sponsorship or charity appeals, without the written agreement of your line manager
- Emails must not be sent or forwarded to a personal email address without prior written authorisation being obtained from your line manager
- If using your own device to access the company's email system/data, you must ensure the device is updated and secure.

If you engage in any prohibited activities this may result in the Auxo Group taking action against you under the Disciplinary & Grievance Procedures and which could lead to the termination of your employment.

Use of networking sites and job boards

Networking sites and job boards are valuable business tools which the Auxo Group wishes to use to build its brand, reputation and business, and which it recognises you may wish to use to build your own professional reputation.

However, in addition to the benefits there are also certain risks attached to using networking sites including but not limited to the Auxo Group's confidential information, reputation and compliance with their legal obligations, including the Data Protection Laws.

When you take professional contact details from job boards or networking sites, this constitutes 'processing' for the purposes of the Data Protection Laws. The Auxo Group must have a lawful basis to process all personal data, including any data taken from job boards and social networking sites.

To reduce those risks, for both you and the Auxo Group, where and when you are representing the company you must comply with the conditions set out in this policy. Failure to comply with this policy may result in the Auxo Group taking action against you under the Disciplinary & Grievance Procedure.

Professional networking sites and job boards

The Auxo Group may provide you with access to professional networking and job board licenses. Such access is granted for work-related purposes only and should be done for the benefit of the company alone, though professional networking activity may be done inside or outside of working hours.

Rules for using professional networking sites

The following rules apply when you access or use a professional networking site or job board:

- You must have written permission from your company Director before requesting an account license for any jobs board or professional networking site
- All account license requests must be submitted to the Group Marketing Manager and Group IT department who will action
- All account licenses must be linked to your work email address only
- Your password is confidential and should not be disclosed to any unauthorised person
- You should only use the account for the purpose for which it was authorised
- If you are commenting on a professional networking site on behalf of the company, you must seek approval from your line manager before submitting that comment
- You shall inform the company of activities that you carry out in relation to professional networking sites or job board including details of your membership of sites that you have set up and new contacts that you have made during the course of your employment

- You must comply with the terms and conditions of use of all networking sites that you use. You should pay attention to any codes of behaviour or professional conduct contained within those terms and conditions
- You must not download or copy professional contacts to any personal device except for a mobile phone and only then if you have been given prior written authorisation from your line manager. No professional contacts should be stored on any other personal storage device. If you have permission to download or copy professional contacts to a personal mobile phone you will give access to the company to those personal devices for audit when requested or if the company receives a personal data request
- You must regularly backup your professional contacts
- You must delete any professional contacts you are instructed to delete by the company (which may include a general instruction to delete records in order to comply with the Data Protection Laws)
- REC Corporate members are also required to comply with the Code of Professional Practice and individual recruiters with the Code of Ethics of the Institute of Professional Recruiters
- You must advise the company if you become aware of any breach of this policy by a colleague. Failure to do so may be a disciplinary offence
- The company reserves the right to restrict your access to professional networking sites and accounts that the company has created for you

Contacts made via professional networking sites

- You must keep personal contacts separate from professional contacts
- The Auxo Group reserves the right to require you to provide evidence and details as to when you made your contacts and in which capacity they were made. You will be required to give access to your account(s) to the Auxo Group Data Protection Officer, Group IT department, your line manager or others for this purpose. The Auxo Group's decision on whether a contact constitutes a personal or professional contact shall be final

Maintenance of company profile on professional networking sites

Certain professional networking sites contain company profile pages relating to the Auxo Group. For the avoidance of doubt, these profile pages may only be created and edited by authorised users. Amendment of the Auxo Group profile pages by unauthorised users shall be a disciplinary offence (and for this purpose you are referred to the Disciplinary & Grievance Procedures).

If you are authorised to make a comment on a professional networking site, you must state clearly whether these are personal views or the views of the Company.

Social networking sites

The Auxo Group respects your right to a private life and therefore you may access social networking sites using the facilities. However, this should be done outside office hours and be kept to a reasonable limit. If there is any evidence that this privilege is being abused, then the privilege may be withdrawn.

Your use of social networking sites may impact on the Auxo Group and its business. Such impact includes potentially causing damage to its reputation, loss of confidential information, or exposure to other liabilities such as claims of discrimination, harassment or workplace bullying. The content of any communications or comments posted on a social networking site must not damage or bring into disrepute the Auxo Group, its staff, clients or candidates. Therefore, if you use social networking sites, even where this is not via the facilities or is outside of working hours you are prohibited from:

- Engaging in any conduct or posting any comments which are detrimental to the Auxo Group

- Engaging in any conduct or posting any comments which could damage working relationships between members of staff, introducers, suppliers, affiliates, clients and candidates of the Auxo Group. Where you express personal views, you must state that these are personal views and do not represent the views of the company
- Engaging in any conduct or posting any comments which could be derogatory to another person or third party or which could constitute unlawful discrimination or harassment
- Recording any confidential information regarding the Auxo Group on any social networking site or posting comments about any company related topics such as its performance
- Making information available which could provide any person with unauthorised access to the Auxo Group, the facilities and/or any confidential information

You may be required to remove postings deemed to constitute a breach of this policy. This may include any 'likes' or 'dislikes' of other people's posts or the re-posting/tweeting of other people's comments (or links thereto) which of themselves may constitute a breach of this policy.

Post termination of employment or engagement restrictions

For the avoidance of doubt, the restrictions on the use of networking sites continue to apply throughout your employment with the Auxo Group including any period of garden leave you may serve.

How to use the facilities and networking sites

Information recipients

You must exercise caution when using the facilities and any networking sites. In addition to the restrictions set out throughout this policy, care must be used in addressing emails, postings on networking sites or other electronic communications to make sure that they are not sent to the wrong individual or company. In particular, exercise care in using e-mail distribution lists or networking sites to make sure that all addresses or site group members are appropriate recipients of the information sent or posted.

Content and tone of communications

All e-mails, postings on networking sites and electronic communications should be courteous, professional, business-like and not contain any material which would reflect badly on the Auxo Group's reputation.

If you receive an e-mail, posting or other communication containing material that is offensive or inappropriate to the office environment then you must inform the Group IT department and delete on their instruction. Under no circumstances should such e-mails, postings or communications be forwarded internally or externally.

If you receive or identify any negative posts on networking sites or social media platforms, you must not reply without consulting the Marketing

Out of office use

If you are out of the office, you should put an 'Out of Office' message on your emails and on your voicemail(s). This message should indicate when you will be back in the office and should identify another person whom the sender or caller can contact in your absence should they need to.

Your emails and phone calls may be monitored in your absence.

Deleting and archiving material

You should not store large quantities of e-mail or downloaded files or attachments. The retention of data utilises large amounts of storage space on network servers, PCs and mobile media, and can adversely affect system performance.

You should delete any e-mails or other communications sent or received that no longer require action or are no longer relevant to your work or to the Auxo Group.

You should retain any information that you need for record-keeping purposes in line with the Auxo Group Data Protection Policy.

Suspect documents, messages or viruses

Any files or software downloaded from the internet, personal mobile media or other software or hardware brought from home (and for which you have previously obtained authorisation to download as detailed in this policy) must be virus-checked before installation on the facilities and use.

If you receive any suspect e-mails, communications, documents or computer virus alerts you should:

- Contact the IT department immediately and without undue delay
- Not open attachments to any email message whose address you do not recognise
- Not forward them to any other internal or external user without the approval of the IT department

Handling misdirected emails

Employees are required to exercise due caution and precision when addressing and sending emails to ensure that all communications are directed to the intended recipients. In the event that an email is mistakenly sent to an incorrect recipient, it is important that the employee immediately notifies the IT department and follows the provided instructions to attempt to recall or delete the email, if possible. Such incidents should also be reported to Business Assurance to assess any potential personal data breach and to determine any further steps to be taken in compliance with the Data Protection Laws and Auxo Group's data protection policies. Failure to do so may result in disciplinary action.

Furthermore, should an employee receive an email that was not intended for them, they must refrain from opening attachments or forwarding the email. Instead, the employee should immediately inform the sender of the error and delete the respective email.

Passwords

Your passwords are confidential and should not be disclosed to any unauthorised person.

The Auxo Group reserves the right to access any accounts (whether email or networking sites) in which case you will be required to give your password to the Auxo Group Data Protection Officer and IT department.

You should use a complex password of either three words or a phrase and include a special character and or number. Please ensure this is something memorable to you. Auxo Group 365 passwords can be changed by you in your account settings or via the forgotten password link. Please ensure MFA options are fully completed to ensure the reset process is efficient. To protect passwords, you should not access the facilities in the presence of others and confidential information should never be left open on the screen when equipment is unattended.

Security

You must ensure that personal data and confidential and sensitive information is kept secure:

- Hard copy files and documents including note pads should be secured when not in use (e.g. locked in a desk drawer) and should be disposed of securely using the shredders or shredding bins provided
- When copying or printing documents you should ensure that documents are never left in meeting rooms, on desks or on the printer
- You should lock your screen when you are away from your desk
- You should ensure that whiteboards do not contain any personal data

- Caution should be exercised when using mobile telephones outside of the workplace
- You are responsible for keeping candidate and client contact details on work mobile phones up to date in line with the data held. If you have photos of candidates or candidate documents on your mobile phone you should ensure these are deleted as soon as they have been passed onto the relevant team or uploaded to the database. Any personal data on mobile phones should not be kept for longer than necessary
- You must not save any files or documents to your desktops
- No external equipment or device may be connected to or used in conjunction with the Company's equipment or systems without the prior express permission of the IT Department

Users are to ensure that all IT devices assigned to, or regularly used by them are used in a manner consistent with their function, so that the possibility of damage and/or loss is minimised.

Portable IT devices must never be left unattended in locations such as airports and hotel lobbies. When devices must be left unsupervised, it must be made as inconspicuous as possible (e.g. equipment should not be left on the seat of an unattended vehicle). Wherever practical, IT equipment will be secured with the supplied security device(s).

IT devices are generally delicate and shall be treated accordingly. Damage to, or loss of IT devices caused by negligence and/or violation of this policy, may result in the responsible party being charged for the repair or replacement costs.

Apart from company owned mobile devices, no other IT devices may be removed from the Company premises without prior written authorisation from the Head of IT.

Users must not modify AUXOIT devices in any manner including, but not limited to:

- Changing the amount of memory in any desktop, laptop, tablet or netbook computers; and

Attaching/installing any peripheral device.

AUXO Password Policy

If you believe your account or password has been compromised;

- You should inform IT immediately
- IT will force a password reset for you
- All accounts should be logged out of and opened again using the new password

File/password protection

When sending internal email with the need to attach documents, these attachments must be sent as links with the appropriate permission set.

When sending an email that contains personal data as defined in the Auxo Group Data Protection Policy, the information must be sent in a password protected format with the password sent by separate email.

Monitoring the use of the facilities, professional and social networking sites

The Auxo Group has the right to monitor any and all aspects of the use of the facilities and any networking sites and job boards and to monitor, intercept and/or record any communications made by using the facilities and any networking sites. This is to ensure compliance with this policy or for any other purpose authorised under the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.

By using the facilities and any networking sites you consent voluntarily and knowingly to your use being monitored. You also acknowledge the right of the Auxo Group to conduct such monitoring.

Unsolicited communications which is not marketing

The Auxo Group must establish that it has a lawful basis to process the individual's personal data before it sends out any non-marketing communication. Any marketing communication must comply with the Auxo Group Marketing Policy.

Termination of employment or engagement with the company

All email address lists or other contact information stored on the facilities are confidential information and remain the property of the company even after the termination of your employment or engagement with the company.

You may not copy or remove any email address lists or other contact information stored on the facilities without prior written permission from the Auxo Group Data Protection Officer and IT department.

You should ensure that any genuinely personal contacts are, where possible, stored separately from any professional contacts. Upon termination of your employment or engagement for whatever reason you may seek permission to remove or copy your personal contacts from the facilities.

On or prior to the termination of your employment or engagement with the Auxo Group for whatever reason you must speak to your line manager to determine what steps to take in relation to any professional networking sites you use. The Auxo Group reserves the right to require you to:

- Advise your professional contacts on any professional networking site of the date on which you will be leaving the Auxo Group and who your professional contacts can contact at the company when you leave
- Delete your account on any professional networking site
- Delete all your professional contacts and not retain a copy of your professional contacts' details without prior written permission from HR
- Hand over control of your account on all or any professional networking sites to the Auxo Group IT department together with all passwords. The Auxo Group IT department, your line manager or other appropriate member of staff will be entitled to notify your contacts on all or any professional networking site(s) of the fact that they have taken over your account.

Employees must be aware that failure to comply with the above rules regarding networking sites could result in disciplinary action or dismissal even if the failure to comply occurs outside the workplace.

Mobile phones

General principles

Staff must use the company mobile phones responsibly, lawfully and in accordance with the terms of this policy.

Company mobile telephones are provided at the company's discretion based on business need and must be returned on the last day of your employment. If staff do not return the mobile telephone and SIM card on the last day of work, we reserve the right to charge you for the cost of a replacement and deductions will be made for the money from the last paid salary.

When returning the mobile telephone and SIM card, all passwords must be supplied or removed from the device.

Eligibility for a company provided mobile phone is determined as an operational matter for managers.

Mobile device management

Certain employees may be issued a company owned mobile device. Use of these devices is contingent upon continued employment with Auxo and the device remains the sole property of the company.

Loss of mobile phone

The safeguarding of a company mobile telephone is the employee's own responsibility. Mobile phones must not be left in a visible place such as in an unattended car. The use of a personal identification number (PIN) must be used for added security.

Loss of a company mobile telephone should be reported immediately to the Auxo Group IT department and/or HR.

If the mobile phone is lost or stolen and the Auxo Group IT department and/or HR are un-contactable (e.g. out of office hours), users should contact the service provider directly to avoid unauthorized use.

To replace a lost handset, the company has the right to deduct the full monetary value of the new phone from your monthly salary.

Voicemail

Employees should ensure their voicemail is set-up as detailed in the instructions supplied with the mobile device. Not only is this convenient, but it is also essential to have this set up in advance in case a call should come in while the mobile phone user is driving.

Etiquette

Employees should be considerate in their use of the company mobile telephone. The device should be turned off when its use could be distracting, for example during meetings and training sessions.

Observe any restrictions imposed by other organisations on the use of mobile telephones, including requests to turn them off.

Redundant or surplus mobile phones

Once a mobile phone has been replaced, upgraded due to age, or becomes surplus, it should be returned to the Auxo Group IT Department at Head Office

Excessive usage

Any excessive charges incurred may result in deductions being made from your monthly salary to cover the amount charged and/or disciplinary action.

Mobile phones & driving

The Auxo Group is committed to reducing the risks which our employees face and create when driving or riding to work.

Employees with a hands-free kit installed in their car should ensure that their use is kept to a minimum whilst driving. You must only take calls whilst driving if it is safe to do so, and you remain in proper control of your vehicle. If circumstances change during the call, you must end the call without delay. You should call back once you have stopped in a safe place and switched off the engine.

Managers must lead by example, both in the way they drive themselves and by not tolerating poor driving practice among colleagues. They must never make or receive a call on a hand-held mobile phone while driving.

Line managers must ensure:

- They lead by personal example
- Employees understand their responsibilities not to use a hand-held mobile phone while driving
- Employees switch phones to voicemail, or switch them off, while driving, or ask a colleague who is a passenger to use the phone
- Employees plan journeys to include rest stops which also provide opportunities to check messages and return calls
- Work practices do not pressurise employees to use a mobile phone while driving

Employees who drive whilst on company business:

- Must never use a hand-held phone while driving
- Plan journeys so they include rest stops when messages can be checked, and calls returned
- Ensure their phone is switched off and can take messages while they are driving, or allow a colleague who is a passenger to use the phone
- With a hands-free kit installed in their car they should ensure that their use is kept to a minimum whilst driving. You must only take calls whilst driving if it is safe to do so, and you remain in proper control of your vehicle. If circumstances change during the call, you must end the call without delay. You should call back once you have stopped in a safe place and switched off the engine

Status of the policy

This policy does not constitute a contract and the Auxo Group reserves the right to change its terms at any time. Failure to comply with this policy may lead to disciplinary action up to and including termination of your employment or engagement with the company.

If an employee has been issued with a company mobile phone, breach of this policy could result in its withdrawal.

Removable media devices

Auxo prohibits the use of all removable media devices. The use of removable media devices will only be approved if a valid business case for its use is developed. There are large risks associated with the use of removable media, and therefore clear business benefits that outweigh the risks must be demonstrated before approval is given.

Requests for access to, and use of, removable media devices must be made to the IT helpdesk before being approved by the Head of IT. Should access to, and use of, removable media devices be approved the following must always be adhered to:

- All removable media devices and any associated equipment and software must only be purchased and installed by the IT department.