



baseGreen

Inspiring • Developing • Empowering



ELECTRONIC COMMUNICATION POLICY



baseGreen



0114 212 5910



hello@basegreen.co.uk
www.basegreen.co.uk



Unit 1, Haggwood Quarry
Honley, Holmfirth, HD9 6PW





POL24-ELEC – Electronic Communication Policy Classification

Document Approval Process		
Document Actions	Completed By	Date
Reviewed and Implemented		5/1/22
Reviewed and rebranded		Aug 24
Next Review		Aug 26

Revision/ Amendments						
Revision number	Section / Paragraph / Page No			Date	Amended by	Comments



POL24-ELEC – Electronic Communication Policy Classification

Document Author	Vonny Broadbent		Role DSL	
Document Owner	Mathew Woodhead		CEO	
	Version No.:	1.0	Date Active:	5/1/22



POL24-ELEC – Electronic Communication Policy

Classification

1. Index

Section No.	Description	Page No.
1.	Index	3
2.	Scope and Application	3
3.	Responsibilities	4
4.	Introduction	4
5.	Email Communication	5
6.	Telephone Communication	8
7.	Video-Conferencing	10
8.	Internet	11
9.	Intranet	13
10.	Monitoring Communications	14
11.	Compliance	15



2. Scope and Application

- 2.1 This procedure applies to all Company personnel and facilities
- 2.2 Failure to comply with the requirements of this procedure may result in investigation and subsequent formal action in line with the Company's Capability and Disciplinary procedures.

3. Responsibilities

- 3.1 **CEO** Has overall responsibility for setting and directing: quality, environmental, safety and health, business continuity and information security policy and for ensuring the appropriate resources are available.
- Is responsible for setting Company objectives and allocating adequate resources to meet those objectives.
- 3.2 **Directors** Are responsible for ensuring that all SMS requirements are established, implemented, maintained and continually improved in accordance with the standards to which the Company subscribes and the legislation relative to the Company's operations.
- Is responsible for ensuring that policies, procedures and associated documentation together with the required systems and associated training are developed and cascaded to individual teams.
- Are responsible for reviewing, issuing and amending all SMS documentation and for providing information and training at all levels of the Company.
- Are responsible for assessing compliance with this procedure during all internal audits.
- 3.3 **Document Owners** Are responsible for all SMS documentation relevant to their department or area of work.
- 3.4 **Document Authors** Are responsible for ensuring that they follow the style guide and process defined within the procedure when producing new or revising existing, SMS documentation.
- 3.5 **All Team Members** Are responsible for ensuring they understand Company policy and procedures and follow the processes at all times.



4. Introduction

Basegreen Academy has adopted the use of many means of electronic communication and information exchange in order to remain competitive, reduce its carbon footprint, and provide staff with efficient tools needed to do their jobs. As a result, staff have access to multiple forms of electronic devices and systems, including computers, landline and/or mobile phones, email, internet, video-conferencing, and the organisation's intranet.

Whilst the organisation encourages the use of these media, all staff should remember that electronic devices and systems provided by the organisation remain the property of the organisation, and that their primary purpose is to facilitate and support its operations.

This document should be read in conjunction with the organisation's Cyber-Security Policy and Data Protection Policy.

Purpose

Whilst it cannot lay down rules to cover every possible situation, the purpose of this policy is to express the organisation's approach and expectations of staff with regard to electronic communication.

It provides instructions and guidance for staff on acceptable usage, recommended practices, and prohibited activities. It also outlines the organisation's right to monitor and access electronic communications.

Scope

This policy refers to all devices, systems and software used by the organisation to send, receive or otherwise create electronic communication. This includes (but is not limited to) the following:

- Laptop, desktop and tablet computers
- Landline and mobile phones (including telephony apps and softphones)
- Email system
- Internet browsers
- Intranet
- Video-conferencing software

This policy applies to all permanent, temporary, contracted and volunteer staff, as well as any other party that is granted permanent or temporary access to the organisation's devices and systems.



5. Email Communication

Sending Emails

- Writing emails: When writing emails, staff should consider the way in which the message is being conveyed to ensure the content is both appropriate and accurate so as not to cause unnecessary misunderstanding.
- Incorrect spelling, grammar and punctuation give a bad impression of the organisation and can make emails difficult to read. Additionally, staff should avoid sending emails in upper-case or bold text as this may be interpreted by the recipient as 'SHOUTING'.
- Selecting recipients: Staff should ensure that emails are correctly addressed and only being sent to people for whom they are relevant. This includes anyone copied ("cc'd") or blind copied ("bcc'd") into the email.
- Forwarding emails: Particular care should be taken when forwarding emails to another person to ensure that all messages contained within the email trail are relevant and appropriate for them to receive.
- Email Signature & Stationery: Staff email accounts are configured with automatic signatures and email stationery (font size, colour etc) during their onboarding process. Staff are not permitted to edit, remove, or otherwise change these default settings without prior consent.
- Disclaimer: All email signatures contain a disclaimer that serves two main purposes: to limit the organisation's potential liability with respect to information being communicated; and to alert recipients that the contents of the email may be monitored and/or disclosed to others.
- Contracts: Staff must be aware that offers, agreements or contracts transmitted via email are as legally binding on the organisation as those sent on paper.
- Sending Personal Data & Confidential Information: Great care must be taken when sending personal data or other confidential information via email. Staff must double-check that they have selected the correct recipient/s, and must ensure that they have permission to share the information prior to sending.
- Any attachments containing large quantities of personal data (e.g., a spreadsheet containing client data that has not been anonymised) should be password-protected prior to sending. Passwords should not be communicated in the same email as the attachments to which they relate, in case the email is intercepted or forwarded to unauthorised personnel.

'All Users' Email Distribution List

In most instances, company-wide news updates and alerts should be communicated via the organisation's intranet rather than via email. Use of the 'All Users' email distribution list by employees is not permitted.

There may be instances where the Directors choose to communicate to all staff via the 'All Users' distribution list rather than through the organisation's intranet. Examples may include (but are not limited to):



- Company-wide updates relating to payroll, pensions or employee benefits
- Communication regarding hazardous weather or other health and safety matters
- Employee illness or death
- Cyber-security alerts

Directors may delegate responsibility for such updates to another member of staff.

Receiving emails

- Response time: Staff should respond to emails within two working days of the date received.
- Spam & Phishing Emails: Whilst the organisation utilises antimalware and anti-spam software to eliminate malicious and 'junk' emails from staff mailboxes, there may be instances where staff receive unsolicited spam or phishing emails. Staff should refer to the Cyber-Security Policy for guidance on how to identify and report such emails.

Automatic Replies (Out of Office)

In the instance of staff absence (including sick leave, annual leave, compassionate leave, and long-term leave), staff should apply an automatic reply to all mailboxes they are responsible for.

If a member of staff is unable to apply an automatic reply themselves (e.g., unexpected absence with no access to email account), their line manager is responsible for contacting the Central Services Manager to apply this on their behalf.

Template automatic replies are available on the organisation's intranet. Staff are not permitted to write their own automatic reply without prior consent from the Central Services Manager.

Managing Emails

- Filing emails: Staff are encouraged to create a folder structure within their Inbox to enable them to organise their emails by subject, client, project etc.
- Deleting emails: The organisation retains emails for three years, before they are automatically deleted. Staff are permitted to delete individual emails ahead of this point, however they are expected to exercise their discretion to ensure that they do not delete emails that may be of operational value.

Staff are not permitted to delete emails relating to the following subjects:

- procurement of services, contract negotiation, or billing
- safeguarding, health and safety, data protection, or cyber-security incidents
- complaints



Personal Use of Emails

- Sending & receiving personal emails: Whilst the organisation's email system is primarily for staff to use for business purposes, limited or occasional use for personal reasons is understandable and acceptable. Staff are expected to demonstrate a sense of responsibility and not abuse this privilege.
- Use of email address for personal activities: Staff are not permitted to use their company-issued email address for any personal accounts or services (e.g., personal social media accounts; online banking or shopping; streaming, gaming or gambling services).
- Use of email address for other business activities: Under no circumstances may staff use their company-issued email address in connection with activities they are conducting on behalf of any other business or entity.
- Use of contacts list for non-work purposes: Staff should be aware that any email contact lists they create are the property of the organisation. As such, contact lists cannot be used for personal or other business activities without the express consent of the Directors.

Misuse of Emails

- Using the company email system for the following purposes is strictly prohibited:
- Gaining access to another member of staff's email folders (or sending an email claiming to come from them) without their permission or the authorisation of the Directors
- Creating or sharing derogatory, malicious, or otherwise potentially defamatory remarks about other persons or organisations
- Creating or sharing discriminatory, harassing, threatening, obscene, offensive, or pornographic content
- Engaging in any other activity that is illegal or contrary to the organisation's policies or business interests

6. Telephone Communication

General Usage

- Greetings: The organisation does not stipulate set greetings that must be used when answering the phone, however staff are expected to incorporate the following elements into their response:
 - A brief salutation
 - The organisation's name
 - Their name
 - An offer of assistance



For example: “Good morning, Basegreen Academy. This is [insert name] speaking, how may I help you?”.

- **Availability:** Staff must ensure that their work-issued phones are switched during working hours. This includes mobiles, desk phones, and softphones (i.e. the Horizon PC Client and Horizon Smartphone app). Connectivity or access issues must be reported via the Equipment Issue Report form swiftly to minimise disruption to internal and external communications.
- **Call management:** Staff should comply with any team-specific targets or guidelines relating to ring time, hold time, call duration, and missed calls.
- **Voicemails:** Staff should listen and respond to all voicemails within two working days of receipt.
- **Speakerphone:** If a member of staff intends to put a caller on speakerphone so that other members of staff can hear them, they must inform the caller before doing so.
- **Text messages:** Staff with company-issued mobiles may communicate with learners, clients and other employees via text message where appropriate. Whilst text messages lend themselves to quick and informal communication, staff must remember that they are still representing the organisation when texting, and should ensure that their messages are clear, polite, and appropriate.

Disclosing Personal Data & Confidential Information

Staff should endeavour to verify the identity of callers prior to discussing or disclosing any personal or confidential information relating to them. Verification checks could include asking the caller to confirm their email address or postcode.

Staff are not permitted to share personal information relating to a client, learner or employee with external callers, unless they have obtained consent from the person to whom the information relates. For example, staff cannot discuss the progress of a learner with their parent, unless the learner has consented to this.

Recording of Telephone Conversations

There may be times where the organisation chooses to record phone calls for internal quality monitoring and training purposes. Recordings will be automatically deleted after 6 months and will never be shared externally without the explicit consent of the participants.

Personal Use of Telephony System

- **Making & receiving personal calls:** Whilst the organisation’s telephony system is primarily for staff to use for business purposes, limited or occasional use for personal reasons is understandable and acceptable. Staff are expected to demonstrate a sense of responsibility and not abuse this privilege.
- **Calls to premium numbers:** Staff are not permitted to use company phones to make personal calls to premium numbers.
- **Use of phone number for personal activities:** Staff are not permitted to use their company-issued phone number for any personal accounts or services (e.g., personal social media accounts; online banking or shopping; streaming, gaming or gambling services).



- Use of phone number for other business activities: Under no circumstances may staff use their company-issued phone number in connection with activities they are conducting on behalf of any other business or entity.
- Use of contacts list for non-work purposes: Staff should be aware that any phone contact lists they create are the property of the organisation. As such, contact lists cannot be used for personal or other business activities without the express consent of the Directors.

Misuse of Telephony System

Using the telephony system for the following purposes is strictly prohibited:

- Making calls or sending texts claiming to be another person
- Creating or sharing derogatory, malicious, or otherwise potentially defamatory remarks about other persons or organisations
- Creating or sharing discriminatory, harassing, threatening, obscene, offensive, or pornographic content
- Engaging in any other activity that is illegal or contrary to the organisation's policies or business interests

7. Video-Conferencing

General Usage

The organisation encourages staff to use video-conferencing as an alternative to face-to-face meetings as this reduces the organisation's carbon footprint and the amount of time staff spend travelling to and from meetings.

When organising or participating in video conferences, staff are expected to behave and present themselves in the same manner that would be expected of them in a face-to-face meeting. Staff should also ensure that any background noise or scenery is appropriate for the nature of the meeting.

Video conferences may be recorded for quality and training purposes, as well as for the purpose of providing a record of the areas discussed. Staff must inform participants if they intend to record a meeting, and recordings must not be shared externally without the express consent of all participants.

Staff must ensure that any sensitive or confidential information on their screen is closed before commencing a screen share during a Zoom / Teams meeting (this includes Outlook web and desktop apps). They should also advise participants to do the same in the instance that they wish to share their screen. If a member of staff believes that they (or a participant) have accidentally shared sensitive/confidential information via Zoom, they must submit a Data Breach / Cyber-Security Incident Report immediately to alert the Data Protection Officer.



Video recording of assessments

Basegreen may at times for the purpose of IQA request recordings of assessment. All recordings should be undertaken on a company issued electronic device. No recordings of lessons/ assessments should be recorded on assessed on a non-company device.

The recordings will be uploaded to a secure drive and then deleted from the original device.

The recordings will only be accessed by authorised personnel.

The length of time the recordings will be stored will be in line with awarding organisation retention requirements.



Conducting Lessons

When conducting a lesson for one or more learners, delivery staff must take the following steps:

- Ensure that their webcam is on, so that the learners are able to both see and hear them
- Ensure that participating learners also switch on their audio and video stream, unless there is a legitimate reason as to why this cannot be done. In such instances, the reason for the lack of audio/video stream should be documented in the learner's OneFile.
- Ensure that the lesson is recorded so that the learner is able to re-watch the content as required, and in order to facilitate the effective quality assurance of teaching and learning

Personal Use of Video Conferencing Systems

Staff are not permitted to use the organisation's video conferencing systems for personal use.

8. Internet

General Usage

- Using the internet to obtain information: Staff must use the organisation's internet facilities sensibly, professionally, lawfully, consistently with their duties and in accordance with the organisation's policies.
- Staff should be mindful that information on the internet may be inaccurate, invalid or deliberately misleading, and any decisions they make based upon it must be subject to scrutiny.
- Reporting inappropriate and/or malicious content: If a member of staff inadvertently accesses an inappropriate and/or potentially malicious website, they should report this to their line manager via telephone or e mail.
- Deleting internet history: Staff are not permitted to delete their internet history or browsing data without prior consent from the Business & IT Analyst; however they are encouraged to routinely delete their cookies, cache and downloaded items to improve the performance of their device/browser.



Social Media

- General usage: Staff are not permitted to use their company-issued email address and phone numbers for the purposes of personal social media accounts. The exception to this rule is LinkedIn (see below).

Staff should refer to the organisation's professional boundaries for guidance on acceptable use of social media both inside and outside of working hours.

- LinkedIn: Staff are permitted to use their company-issued email address and phone number on LinkedIn, provided that their profile makes clear reference to their position at the organisation.

If staff wish to use the organisation's branding on their profile, they should contact Marketing to obtain the appropriate imagery.

Staff may wish to connect with clients and learners via LinkedIn, however they should note that such communication falls within the scope of this policy. Staff should refer to Email Communication: Sending Emails (see above) for guidance on acceptable use.

Online Forums

The organisation recognises that participation in some forums may support a member of staff's performance of their job role. For instance, they may find the answer to a technical problem by consulting members of a group devoted to the technical area in question.

Staff should include the following disclaimer in all posts made in public forums:

"The views, opinions, and judgements expressed in this message are solely those of the author. The message contents have not been reviewed or approved by organisation."

Employees should note that even where disclaimers are used, a connection with the organisation exists and a statement could be imputed legally to the organisation. Therefore, employees should not rely on disclaimers as a way of insulating the organisation from the comments and opinions they contribute to forums. Instead, employees must limit their discussion to matters of fact and avoid expressing opinions that could bring the individual or company into disrepute.

Communications must not reveal information about the organisation's processes, techniques or trade secrets, or divulge any other confidential information, and must not otherwise violate the organisation's policies.



Personal Use of the Internet

Whilst the organisation's internet service should primarily be used for business purposes, limited or occasional use for personal reasons is understandable and acceptable. Staff are expected to demonstrate a sense of responsibility and not abuse this privilege.

Staff should be aware that the organisation reserves the right to monitor internet usage (see Monitoring Communications below). As such, staff must be mindful that by using company-issued devices/browsers to use the internet for personal activities, they may inadvertently reveal sensitive and personal information about themselves. For example, if a member of staff regularly uses company devices to visit websites which detail the activities of a particular political party, religious group or trade union, it may indicate their own political opinions, religious views, or trade union membership.

Misuse of the Internet

- Using company-issued devices to access and use the internet for the following purposes is strictly prohibited:
- Online gambling
- Creating or sharing derogatory, malicious or otherwise potentially defamatory remarks about other persons or organisations
- Creating or sharing discriminatory, harassing, threatening, obscene, offensive or pornographic content
- Engaging in any other activity that is illegal or contrary to the organisation's policies or business interests

9. Intranet

Staff should refer to the company code of conduct for guidance on acceptable communication and prohibited activities related to the organisation's intranet system.



10. Monitoring Communications

Monitoring System Access & Usage

The organisation is ultimately responsible for all electronic communications sent via company systems and/or devices, but subject to that will, so far as possible and appropriate, respect the privacy and autonomy staff while working.

However, it should be noted that the organisation may compile activity logs of electronic system usage for the following purposes:

- Cost analysis
- Resource allocation
- Optimum technical management of information resources and systems
- Providing intelligence during the procurement of new systems
- Detecting patterns of use that indicate staff may be violating the terms of this policy or engaging in illegal activities

Accessing Electronic Communications

The organisation reserves the right, at the discretion of the Directors, to access and review any member of staff's electronic files, emails, texts, internet history or system activity for the following purposes:

- Ensuring electronic media and services are being used in compliance with the law and the organisation's policies
- Obtaining evidence of business transactions
- Looking for information in response to a request for information under data protection or freedom of information legislation
- Monitoring standards of service and staff performance, and identifying staff training needs
- Accessing urgently-required information in the instance of staff absence



11. Compliance

Line managers must ensure that new staff are made aware of this policy before they are permitted to start using the organisation's electronic communication systems.

Staff who abuse the privilege of access to electronic communication systems facilitated by the organisation face being subjected to disciplinary action, up to and including termination of employment. They also risk having the privilege removed for themselves and possibly other staff.

This policy does not form part of the contract of employment and any or all of its terms may be amended from time to time.



baseGreen
Inspiring • Developing • Empowering