IT ACCEPTABLE USE POLICY

BADGER GROUP
Badger House
121 Glover Street
Birmingham, B9 4EY

Destroy All Previous Issues

Contents

DOCUMENT CONTROL

Document Storage

Location: p:\ops team\central policies & procedures - development - word docs\it policies\it-po-02 it acceptable use policy v1.1.docx

Version Control Log

(Only last 3 versions, earlier versions can be found in the appropriate archive directory for the document)

Version	Date	Author	Description of Changes
V1.0	July 2022	Doc Control	Original version was previously HR-09 (HR Policies) it was agreed this should come under IT with immediate effect
V1.1	Jan 2023	Waqar Azmi	Update to section 3

Approval

Version	Name	Position	Signature	Approved Date

Glossary

Term	Description

1 INTRODUCTION

This document outlines Badger's IT policy that applies to all staff.

Badger has prepared this policy to provide guidance in respect to the use of, and the security of, Badger's information technology. This includes the sending and receiving of email. Guidelines however cannot replace judgment, interpretation and analysis of specific situations.

Badger depends on its computer systems (both hardware and software) for the efficient operation of its business. The use of computers and information technology carries risks, as well as benefits. Badger has therefore established certain rules to minimise the risks to its business from the use of its computer systems and also the use of electronic mail.

All employees are required to observe the rules in this document at all times. Any serious or persistent breach of the rules will be deemed as gross misconduct and liable to summary dismissal.

2 SECURITY OF COMPUTER SYSTEMS PROGRAMS AND DATA

2.1 General – computer viruses and basic protective measures

A computer virus is a piece of alien software, written for mischievous or malicious purposes, which attaches itself to other software on a system and is then triggered by a particular event in order to cause chaos. When a virus is introduced to a network (such as Badger's network), then the effects can be very widespread and disastrous. A common means of introducing a virus into a computer system is via the internet, by email (with attachments), by data-key (USB key) or by CD and particularly those containing computer games. New viruses are being created all the time and there is no guarantee that Badger's virus protection software is capable of detecting every virus.

In order to protect Badger's systems, the use of computer games on Badger's systems is strictly prohibited and all users who receive software, such as games and puzzles, by e-mail must:

- If practicable, inform the sender that the receipt of such e-mails and attachments on Badgers computer systems is strictly prohibited; and report the receipt of the e-mail to a member of the IT team or the Director of Operations.

- All external devices such as USB pen drives, cd's and external hard drives should have a virus scan before being introduced to the Badger network. The scan can be run on the device by the Technical Team to insure it is safe to use.

- Do not attempt to open or otherwise deal with the software; and under no circumstances further distribute the software around Badgers computer system, as this could result in any virus being spread over many PCs , alert a member from the technical team ASAP

2.2 Prohibited activities in any circumstances

The following activities are **strictly prohibited** in any circumstances:

2.2.1 Accessing, downloading, importing, retaining or communicating data (documents, software, information, images or other materials) that is unauthorised or unlawful or in violation of Badgers policy, including (but not limited to) data that is (or could reasonably be considered to be) pornographic, defamatory, obscene,

(i.e. contain nudity), violent, sexist, ageist, homophobic, religious, racist, hate-related or associated with terrorist activities.

2.2.2 Copying or transmitting data protected by the copyright and related laws, without copyright or similar authorisation.

2.2.3 The unauthorised use of passwords to gain access to another users information or communications.

2.2.4 Electronic "snooping" i.e., to satisfy idle curiosity about the affairs of others, with no business reason for obtaining access to the files or communications of others (this prohibition applies to all users, including personnel with Systems Administrator's rights and Supervisors); electronic 'snooping' includes but is not limited to 'hacking' into the voicemail, electronic mail, or other data addressed to others within the company's communication systems.

2.2.5 Knowingly introducing a computer virus into Badgers communication systems and any other non-compliance with Badger's rules and guidelines concerning the avoidance of computer virus.

2.3 Prohibited activities except with written permission

Except to the extent that they form part of the duties of your employment, the following activities are **strictly prohibited** without the prior written permission of the business support manager and Director of Operations.

2.3.1 The installation or removal of application software or data files to or from either the network drives or local drives of the PC computer system;

2.3.2 The installation of demonstration CDs to either the network drives or local drives of the PC computer system;

2.3.3 The carrying out of any programming on any part of Badger's computer system;

2.3.4 The introduction of any computer games software onto any part of Badger's computer system;

2.3.5 The revelation of any identification code or password between staff, or to any other person.

2.3.6 Access to the server room unless in the presence of authorised support staff;

2.3.7 Leaving your PC or laptop on overnight, exposing it to the risk of undetected unauthorised access;

2.3.8 Copying software products purchased by Badger onto computers not owned by Badger and the making of a secondary copy of software for use on any computer not owned by Badger (including laptops and home computers).

2.4 Who is permitted to use the Badgers computer systems?

You are a permitted user of Badgers computer systems if, and to the extent that, the proper performance of the duties of your job requires you to have use of the systems. Use of Badgers computer systems for other purposes, for example receiving and sending personal e-mails or personal use of the Internet, is **discouraged** in working hours except for the following permitted purposes.

2.4.1 For examinations.
Badger recognises that staff may wish to use Badgers computer systems for support in their studies for professional and other examinations and this is permitted

2.4.2 For personal use.
Badger recognises that from time to time personal circumstances may permit that Badger's email system is used for incidental and occasional personal use. Such use is permitted in situations (where it is necessary that you contact a relative or partner by email because you cannot contact them by another means outside working hours) provided it is not habitual or frequent in nature.

2.4.3 For business development.
Badger is keen for staff to develop a good understanding of the Internet in order to be able to talk knowledgeably about its uses to external contacts. It is therefore recognised that it is reasonable to use the Internet for this purpose provided that it is confined to sensible use. Any such use should not contravene any of the prohibited uses detailed above.

You are permitted to use Badgers Internet and email system for personal use outside your normal working hours subject to such use being reasonable in terms of both the amount of time you spend on Badgers Internet and email system and subject to you complying with all other aspects of this policy.

Badger considers that up to one hour per day would constitute reasonable personal use.

The use of Badger's computer and email system may be monitored by Badger **AT ANY TIME** – including personal use, to police compliance with this policy and rules which are subject always to Badger's wish to comply with all relevant legislation including the Data Protection Act 1998.

Compliance with the policy will be subjected to regular audits, on no less than a monthly basis, which will focus on (but is not limited to) large downloads, content of images stored and contents of text stored.

Failure to follow this policy may ultimately invoke disciplinary procedures which could result in your dismissal from employment.

Staff should seek prior written permission from the Director of Operations if they wish to use Badgers computer system or email for any purpose not permitted by this policy.

2.5 Use of unlicensed software

It is an offence to use unlicensed software. Therefore, unlicensed software must not be used on Badger's computer systems.

2.6 Email Access

2.6.1 Potential risks/dangers of using e-mail

Email has the advantage of convenience but the use of it also carries significant risks.

For example: email encourages a degree of informality that may not always be appropriate to the circumstances and may give rise to unforeseen consequences;

An e-mail is an electronic file that can be amended by the recipient and, having been changed, it could then be passed to a third party who would be unaware of the changes;

An e-mail has the same legal status as a letter. It is possible to libel a person in an e-mail in the same way as in any other written communication.

A breach of copyright will occur if a document is copied without the permission of the copyright owner;

The sender cannot be sure who will read the e-mail;

The sender and recipient cannot be sure when the e-mail will be received or read. This depends partly on the type of e-mail account maintained by the recipient, the time of day it is sent and other factors; e-mail is a common source of importing viruses into the computer system.

2.7 Minimising the risks – Badgers rules for the use of e-mail

In order to minimise the potential risks to Badger arising from the use of e-mail, Badger has established the following rules in respect of both internal and external e-mail. You are required to observe these rules when you send and receive e-mail using Badger's computer systems, or when working on Badgers business:

2.7.1 E-mails may only be sent or received on Badger business. Personal e-mail messages, whether internal or external, may not be sent or received unless permitted elsewhere in this policy. If you are sending an email which is permitted under this policy you should mark the email 'Personal' in the title and request that any response is similarly marked. Badger is entitled to assume that all emails which are not marked 'Personal' are emails relating to Badger and its business and can be viewed accordingly even after your employment with Badger has ended.

2.7.2 If you receive unsolicited e-mail, that does not relate to Badgers business or your job, you must immediately notify the sender that such e-mails are not permitted, must not be sent in the future and will be deleted unread. On no account may any attachment be opened or may the message or attachment be forwarded to any other person.

2.7.3 You must not say anything in an e-mail that you would not be prepared to say in a letter (on Badgers headed paper) sent to the same person. For example, you must not generate or send e-mails that contain explicit, offensive or obscene material or language or that contains material that is defamatory or could be construed as constituting sexual, ageist, homophobic, religious or racial discrimination or harassment.

2.7.4 Sending, forwarding, redistributing or replying to "chain letters".

2.7.5 In all cases you must be aware of the dangers of excessive informality. Never assume a position of informality in your e-mail. Even if you have made good friends at work and are emailing them on a more social level you should clearly distinguish between the language you might use for the 'do you fancy meeting for lunch' emails and the 'please could we meet to discuss your proposal' emails. There may be a time when one of you needs to forward the work email to another colleague and therefore regrets the informal tone and it helps to differentiate between your professional relationship and your friendly one.

2.7.6 E-mails are not confidential, even with password protection, and can be read by other users. Therefore, confidential company information must not be sent by e-mail (whether internal or external) except with the prior written permission of the Director Of Operations who will also advise on the correct encrypted form to be used.

2.7.7 If a stand-alone computer has received an e-mail with for an example a program in form of an e-mail (e.g. a game) under no circumstances this program should be launched. You must inform the IT department or the Director of Operations of the program's arrival.

2.7.8 You must divert your e-mails, or set up an appropriate 'out-of-office' message when absent or otherwise off-line for a prolonged period of time. If you intend to reference other people in your 'out-of-office' message, permission should be sought in advance from them.

2.7.9 If you receive an unsolicited email which you suspect may be in breach of anything contained in this policy, you may forward it to either the Director of Operations or the Human Resources Department without that particular action breaching the rules of this policy.

2.8 Email good practice

2.8.1 Make emails as short and to the point as possible.

2.8.2 Do not type in CAPS unless there is a specific point to be made as this is considered shouting on-line. Various studies on the topic of e-mail etiquette reflect that it is more difficult and takes longer to read an email that is typed all in CAPS.

2.8.3 Pick distribution lists carefully. Consider whether all those receiving the Email will *really* be interested. Use your better judgment when using the 'Reply to All' feature. In many instances, your comments may not be appropriate for "all" or "all" may not be interested in your comments. Make a point of reviewing those who will receive your reply and use your discretion. That way it will be a conscious choice to include, not a 'default' action.

2.8.4 Angry emails'. Do NOT respond immediately. It is always better to wait until you have absorbed any initial irritation and then if possible speak to the sender in person. This will enable misunderstandings to be clarified and also demonstrates that you are keen to deal with the content proactively.

2.8.5 Use discretion. It is all too easy to copy senior Badger Managers into emails in order to try to impress, or hurry the main recipient, or because you want to inform senior staff. However this can be irritating to both the senior manager who is getting emails they don't need, and to the recipient who may feel they have been exposed or pressurised by your actions.

2.8.6 An email copied to a person means no action is required on their part.

2.8.7 Avoid using complex formatting in your emails. For example using bold orange letters or flashing type makes your email look like spam and therefore may be filtered accordingly.

2.8.8 Do not leave the subject field blank. This is important as it helps those you communicate with to organise and manage their email.

2.8.9 The corporate font at Badger is Arial and this should be used for all day to day paper and electronic documents.

2.8.10 If you have any questions about this policy or its interpretation then please discuss your concerns with either your line manager, a member of the HR Department, or the Director of Operations. In the event of disciplinary proceedings being instigated for a breach of any of the rules contained within this policy, ignorance of the policy will not be accepted as a valid argument.

2.8.11 If sending an e-mail to a wide range of people for example doctors or external companies some people do not wish to have their e-mail address on view. Please use the bcc option for privacy.

2.9 Internet Usage

The Badger network has now had a smartfilter installed, what smartfilter does is monitors internet activity by users throughout the company. If any words which appear within the block list are accessed by the user while surfing the internet the technical team will have an e-mail sent.

2.9.1 Employees should lock their computer to insure that other users do not surf the web using that employees account.

2.9.2 If someone is surfing a website which they shouldn't be then the technical team should be made aware are so action can be taken.

2.9.3 If a member of staff has accessed a site which is of sexual nature this will be classed as gross misconduct (see policy relating gross misconduct)

2.9.4 Accessing, downloading, importing, retaining or communicating data (documents, software, information, images or other materials) that is unauthorised or unlawful or in violation of Badgers policy, including (but not limited to) data that is (or could reasonably be considered to be) pornographic, defamatory, obscene, (i.e. contain nudity), violent, sexist, ageist, homophobic, religious, racist, hate-related or associated with terrorist activities.

2.10 Instant Messenger

Instant Messenger' is a module within the Adastra application which allows users to send messages to other users who have logged into the Adastra system.

Messages may only be sent or received on Badger business; personal messages may not be sent or received under any circumstances. If you receive any personal message on the instant messenger module, you must notify the sender that such messages are not permitted and close the module not to continue with the conversation.

Messages are not confidential and can be viewed by the management team and regular audits are carried out to ensure compliance with the policy.

Instant message is an informal method of passing information, however you must not say anything in the instant message that may that contain explicit, offensive or obscene material or language or that contains material that is defamatory or could be construed as constituting sexual, ageist, homophobic, religious or racial discrimination or harassment.

In all cases you must be aware of the dangers of excessive informality. Never assume a position of informality in your message

It is the responsibility of managers to ensure that their employees are very aware of Badgers expectations in terms of the management of its computer systems and the required adherence by staff to this policy. It is suggested that managers issue a copy of this policy to every employee.

3 ACKNOWLEDGEMENT – PRINT THIS PAGE, SIGN AND RETURN:

Scan and email to training@badger.nhs.uk

I acknowledge that I have read the IT Acceptable Use Policy document, and agree to abide by the policy.

Signature

Full Name (Printed)

Role

Date