EMAIL 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\IG - IGSoc - GDPR Policies\IG-37 - Email Policy V2.2.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
V2.0	April 2021	S Owen	Reviewed, no changes
V2.1	April 2022	S Barnes	Reviewed, no changes
V2.2	May 2023	Suzanne Lurie – DPO, Regulatory Solution	Reviewed, no changes

Approval

Version	Name	Position	Signature	Approved Date
V1.5	IGSG	IG Steering Group		14 Mar 2018
V1.6	Badger Executive	Executive Tea,		25 July 2019

Glossary

Term	Description

1 INTRODUCTION

This policy details the framework within which Badger Group supports the use of email. The policy has been developed in conjunction with the NHS Digital guidelines and the latest version of exemplar materials.

This policy supports the Badger I.T. Acceptable Use Policy. The purpose of this policy is to ensure that email is used appropriately across Badger.

This policy contains important rules covering email. Many of the rules apply equally to Badger's other methods of external communication such as letter, the use of fax and telephone.

The use of Badger equipment to access non-Badger personal email accounts via the internet is strictly forbidden without the exceptional approval of the SIRO and/or IG Lead. Accessing personal email accounts using Badger equipment can compromise cyber security and has potential to introduce a virus that could compromise the network and access to Badger systems. Non-compliance will be referred to Line Management and a serious incident form raised for investigation.

Commented [SO1]: We need to get this section front and centre for all staff along with the rule about not plugging in personal equipment

1.1 Definitions

Spamming **-** Spam is unsolicited commercial email, the electronic equivalent of the junk mail that comes through your letterbox.

Phishing **-** Phishing is the use of bogus emails and websites to trick an email user into supplying confidential and personal information.

Chain Letters **-** A chain letter is an electronic email that urges you to forward copies to other people.

Ephemeral **-** Ephemeral email is email which facilitates Badger business but does not need to be retained for business purposes.

2 LOCATION

This policy is applicable to all staff, contractors and volunteers using Badgers email systems.

3 RESPONSIBILITY

3.1 All staff using email

It is the responsibility of all staff to comply with this and all other IT policies.

When sending an email that contains one or more personal email addresses you should always default to using the 'bcc' (blind copy) to circulate the email. This prevents personal email addresses being shared with others where explicit consent has not been provided. If a personal email address is shared without consent this becomes a breach of confidentiality under the Data Protection Act 2018 (UK GDPR).

Email users should be aware that they neither own the documents that they or their colleagues create, nor have intellectual property rights therein.

3.2 IT Department

The Information Technology (IT) Department will monitor the use of the Email systems. All Email is stored and Badger may inspect email without notice. Some of the most likely reasons for monitoring email are:-

- Checking to see if email is related to business;

- Checking the quality of service;
- Making sure email is operating properly; and
- Preventing or detecting crime.

The IT Department will notify the Line Manager and Human Resources Department of any breaches of this policy

3.3 Line Managers

It is the responsibility of Line managers to ensure that all staff are aware of and adhere to the contents of this policy.

Responsibility for taking any appropriate disciplinary action following a breach of this policy lies with the relevant Line Manager having taken advice from Human Resources Department.

4 OPERATIONAL SYSTEM

4.1 When to use Email

It is the responsibility of the person sending an email message to decide whether email is the most appropriate method to communicate the information. The decision to send an email should be based on a number of factors including:

- The subject of the message;
- The recipient's availability;
- The speed of transmission;
- The speed of response required;
- The number of recipients of the email.

4.2 Writing Business Email Messages

When writing a business email message it is important that consideration is given to the way in which the message is being conveyed. This includes thinking about the title, the text and the addressees. Refer to the email good practice guidelines. (Appendix 1)

Email messages constitute a formal record and can be used as evidence in legal proceedings.

4.3 Personal Use

Badger defines reasonable personal use as 'transactions of personal affairs' which cannot be avoided during working hours.

Staff who have access to Badger email for business purposes may make reasonable personal use of email facilities provided by Badger. The personal use should be kept to a minimum and is permitted only during authorised break times where it:-

- Does not interfere with the performance of your duties;
- Does not overburden the system;
- Does not create any additional expense to the organisation.

The conditions of this policy also apply to personal use of email.

4.4 Security

Each Email account, whether a personal or group account, is protected by network, user and password security.

Individual users must take personal precautions to ensure the security of their email account including locking the PC before leaving it unattended. This will prevent others reading your email or sending a potentially embarrassing hoax message in your name.

It is possible to permit other email account holders to open your mailbox or send email on your behalf. Contact the IT Service Desk if this is required.

Archiving: The storing of personal data (within the meaning afforded to it with the Data Protection Act 2018) is subject to the same controls as any other personal data and is therefore subject to Subject Access Requests.

Virus Protection: The most common way of receiving a computer virus is through email. Software has been installed on the Email servers which scans each email attachment for embedded viruses as soon as it enters the Network.

At individual level it is the responsibility of all email account holders to:

- Delete any messages from unknown origin;
- Contact the IT Service Desk immediately should they receive notification that en email sent to or by them contains a virus.

4.5 Confidentiality/Sending Patient Identifiable Information

Badger accepts that NHSmail is the only method by which Personally Identifiable information can be securely sent by email.

The majority of Badger email users are using locally provided email accounts, i.e. firstname.surname@badger.nhs.uk These accounts must not be used to send/receive personally identifiable information; this includes patient and staff data The Medical Director acting in the capacity of Caldicott Guardian and the Director of Service Delivery acting as the Senior Information Risk Officer (SIRO) have NHSmail accounts. All email containing personally identifiable information must only be sent/received by these accounts.

When using NHSmail, Personally Identifiable Information can be sent to the following addresses ensuring confidentiality

- nhs.net
- gsx.gov.uk
- gsi.gov.uk
- gse.gov.uk
- pnn.gov.uk
- scn.gov.uk
- pnn.police.uk
- eu-admin.net
- gsisup.co.uk
- cjsm.net
- psops.net
- cjs

Where personally identifiable information must be transmitted to external organisations, there is a much greater risk of unencrypted emails being intercepted with a consequent breach of patient confidentiality.

Only NHSmail accounts may be used to send personally identifiable information to external recipients who use the secure email addresses noted above.

It is not acceptable to send personally identifiable information externally from Badger by another route.

4.6 Emailing Patients

Personally identifiable information can be sent to patients via a Badger email address as long as the patient has consented and has been made aware of the potential risk.

4.7 Misuse and Abuse of Email

The sending of email which can or does cause distress will be dealt with by the appropriate Badger HR policy.

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 IG Lead or the Human Resources Department without that particular action breaching the rules of this policy.

The transmission of any kind of sexually explicit image or document is expressly forbidden. If you need to transmit sexually explicit images or documents for a valid clinical reason, the permission of the Caldicott Guardian must be sought in advance.

Behaviour or comments that are not permitted in the spoken or paper environment are also not permitted in email messages.

Email messages containing inaccurate information in the form of opinion or fact about an individual or organisation, may result in legal action being taken against the person sending the email message and anyone forwarding the email message on to others.

4.8 Training

Email and acceptable use of IT forms part of the Badger Induction programme that is mandatory for all staff.The module is delivered by the Training Department to all new starters in Badger.

All staff are required to participate in mandatory annual Data Security & Protection training as part of Badger's Data Security & Protection Statement of Compliance.

4.9 Housekeeping

It is the responsibility of all members of staff to manage their email messages appropriately. It is important that email messages are managed in order to comply with Data Protection legislation.

To manage email messages appropriately all Badger staff must identify email messages that are records of their business activities. Clinical or managerial records should be moved from personal mailboxes and managed in the same way as other records.

Ephemeral email messages should be managed within the mailbox and kept only for as long as required before being deleted.

A storage limit is set on all email boxes. You will receive a warning message informing you when you are reaching your limit.

Emails must be deleted on a regular basis – this includes inbox, sent items and deleted items.

4.10 Global Email

Caution should be exorcised when sending global emails to large groups of personnel. You need to consider whether it is appropriate to broadcast the email address of all those included in the To/CC address lines. You should also consider the consequences of "Reply to All" being selected in response to the mail and whether it is appropriate in respect of the content of the mail.

4.11 Unsolicited Email (spamming)

Badger's Email system is protected from 'spamming' and NHSMail users can setup filters both of which can prevent unsolicited mail.

"SPAM" Mail can be avoided by the following:

- If you don't know the sender delete the email;
- Never respond to spam or click on links within it;
- Never give your email address on the internet;
- Only give your email address to people you trust;
- Use the 'bcc' field if you email many people at once;
- Never make a purchase from unsolicited email.

4.12 Hoaxes, Scams & Chain Letters

If you receive any form of the above in emails do not forward them to anyone, delete them immediately and inform the IT Service Desk

4.13 Accessing the Mailbox of another Member of Staff

There may be occasions when it is necessary to access email messages from an individual's mailbox when a person is away from the office for an extended period, for example sick leave. The reasons for accessing an individual's mailbox are to action:

- Subject access request under the Data Protection Act;
- Evidence in legal proceedings;
- Line of business enquiry;
- Conducting an investigation which may result in disciplinary action.

Where it is not possible to ask the permission of the member of staff whose mailbox needs to be accessed, the procedure for gaining access to their mailbox is:

- Gain authorisation from the Head of Department;
- Submit a request to the SIRO or IG Lead;
- A record will be made of the reason for accessing the mailbox together with the names of the people involved; (IG-37-ERR – Email Request Register)
- Inform the person whose mailbox was accessed.

It is less likely that this procedure will need to be followed if mailbox access has been delegated to a trusted third party.

4.14 Shared Mailboxes

Shared mailboxes should be used where there is a group of people responsible for the same area of work to ensure that queries are answered quickly when members of the team are away from the office.

Access to a shared mailbox must be authorised by a member of the Exec Team before IT Department undertake the work. Access can also be granted by the person who owns the mailbox but must receive Exec approval.

4.15 Public Mailbox Folders

The public folders are accessible by everyone using Badger email systems (other than NHS mail users) and are organised into folders.

The public folder should be used for people across Badger who want to share ideas relating to a particular area of work.

4.16 Disclaimer

A Badger disclaimer is appended to every email message sent from the Badger email system (this does not apply to the NHS mail email). It should include information about how to send personally identifiable information.

4.17 Summary

- **DO** attend an email training session;
- **DO** protect the Security and Confidentiality of the system and information;
- **DO** regular Housekeeping;
- **DO** read and action the email good practice guide;
- **DO NOT** misuse or abuse the system;
- **DO NOT** email anything that could result in criminal or civil prosecution, or which could lead to disciplinary proceedings against you;
- **DO NOT** send a Global Email without careful consideration

5 RISK MANAGEMENT

Failure to abide by this policy could lead to breach of the Data Protection Act, and Caldicott recommendations.

It is the responsibility of the Line Manager to ensure this policy is deployed within their area of responsibility.

6 RELATED DOCUMENTS

HR-22 - IT Acceptable Use Policy
All other supplementary Badger IT Security Policies

7 REFERENCES

Data Protection Act (2018)
Human Rights Act (1998)
Regulation of Investigatory Powers Act 2018

8 APPENDIX 1

EMAIL GOOD PRACTICE GUIDELINES

1. EMAIL ETIQUETTE

Who are you?

It is good practice to identify yourself and your position at the end of the email. This may not be apparent from your e-mail address alone. The email systems in use in Badger allow the creation of Signature Files that can be attached to the end of each email message.

Email formatting and content

- Badger email format is:-
  - Blank background
  - Font – Arial 11
  - Auto signature containing – name, job title, telephone number, fax number (see below for Badger standard signature)

badger
CARE YOU CAN TRUST
Full Name, Surname
Job Title
Badger Group

DDI: XXXX XXX XXXX
FAX: XXXX XXX XXXX
Website: www.badger-group.com

This e-mail and any files transmitted with it are confidential. If you are not the intended recipient, any reading, printing, storage, disclosure, copying or any other action taken in respect of this e-mail is prohibited and may be unlawful. If you are not the intended recipient, please notify the sender immediately by using the reply function and then permanently delete what you have received.

- Always ensure the e-mail SUBJECT line is completed;
- Internal email can increase the effectiveness of interpersonal communications with colleagues and can improve efficiency in creating, editing and accessing written documents.
- Electronic communication out with Badger represents an outstanding opportunity to improve the speed and efficiency with which we communicate with our working partners. It also raises important issues in the areas of data security, confidentiality and interpersonal communications.

2. EMAIL GOOD PRACTICE

- Be careful about disclosing confidential information, remember that email can be easily copied and forwarded.
- Be vigilant when receiving files attached to email, especially from unknown sources, such files often contain viruses. If you are unsure, do not open the file and contact the I.T. Service Desk.
- NEVER disclose your password to anyone. Nobody has the right to know your personal password, and if you divulge it to another, both of you will be in breach of the I.T. Security Policy and may be liable to disciplinary action. Please refer to the Badger Password Management Policy (Ref IG-26)
- Check email on each working day or arrange for a duly authorised person to do so.
- Advise people when you are not available. When out of the office and not able to log into your mail account, use the tools within the system to notify others of your inability to do so.

- Reply promptly to all email messages requiring a reply.
- Request confirmation of receipt on important emails sent, when requested recipient should acknowledge receipt.
- Notify your line manager or Human Resources department if email is received which is regarded as illegal or offensive.

3. GUIDELINES FOR WRITING BUSINESS EMAIL MESSAGES

Subject Line

- Ensure the subject line gives a clear indication of the content of the message.
- Indicate if the subject matter is sensitive.
- Use flags to indicate whether the message is of high or low importance.
- Indicate whether an action is required or whether the email is for information only.

Subject and Tone

- Greet people by name at the beginning of an email message.
- Ensure that the purpose and content of the email message is clearly explained.
- Include a signature with your own contact details.
- Ensure that the email is polite and courteous.
- Make a clear distinction between fact and opinion.
- Proof-read message before sending.
- Include original email message when sending reply.
- Ensure email messages are not unnecessarily long.

Structure and Grammar

- Try to use plain English.
- Check spelling before sending.
- Put important information at the beginning.
- Avoid abbreviations.
- Avoid using capital.
- Do not use emoticons.

Addressing

- Distribute email message only to the people who need to know the information.
- Think carefully before using reply all.
- Use 'To' field for people who are required to take further action and the 'cc' field for people who are included for information only.
- Ensure email message is correctly addressed.

General

- Be aware that different computer systems will affect the layout of an email message.
- Avoid sending messages in HTML format as if an email recipient is using an email system that does not support HTML the layout will be affected.
- Be aware that some computer systems might have difficulties with attachments.
- Observe the restriction of the attachment i.e. 2mb.
- Try not to forward messages unnecessarily.

9 EMAIL REQUEST REGISTER

Date Request for Email Access Received	Requested by	Name of staff member whose emails have been requested	Reason for request	Name of staff member granted access	Date/Time Access Given	Date/Time Access Removed