Email guidelines for the Bar

Purpose:	To guide all barristers and chambers on good practice in their use of email and email security
Scope of application:	All practising barristers
Issued by:	The Information Technology Panel
Originally issued:	November 2004
Last reviewed:	July 2024
Status and effect:	**Please see the notice at end of this document. This is not "guidance" for the purposes of the BSB Handbook I6.4.**

Acknowledgement

The Bar Council Email Guidelines are substantially based on those adopted by the Law Society which in turn worked with the Bar in drafting its own March 2004 guidelines.

Introduction

1. The benefits of email to businesses and individuals are incalculable. As an internet application, email can be used in both secure and insecure ways, thereby exposing barristers and their chambers to certain risks. These include the risk of failing to comply with various statutory requirements, for example, data protection legislation, and threats to the security of IT systems.

2. Consideration should be given to the security features available to you and, particularly where you are processing personal data, you must take appropriate technical and organisational measures in order to ensure that your email communications are safeguarded.

3. This document sets out best practice guidelines for your professional conduct as relates to email and email security. A draft model email policy, which chambers can tailor to their requirements, is also set out in Annex A.

Professional Conduct

4. Barristers and chambers must have regard to their Core Duties under the BSB Handbook, particularly CD5, CD6, CD7 and CD10 when considering best practice as relates to email and email security:

> CD5 You must not behave in a way which is likely to diminish the trust and confidence which the public places in you or in the profession.
>
> CD6 You must keep the affairs of each client confidential.
>
> CD7 You must provide a competent standard of work and service to each client.
>
> CD10 You must take reasonable steps to manage your practice, or carry out your role within your practice, competently and in such a way as to achieve compliance with your legal and regulatory obligations.

Timely responses

5. A barrister should deal promptly with communications relating to instructions.

6. Arrangements should be made to check incoming emails during periods of extended or prolonged absence.

7. Barristers and chambers should consider using automated out-of-office responses when someone is away from chambers for a day or more.

Maintaining records

8. Barristers and chambers should take a pragmatic and common-sense approach to records of emails. That is, significant and substantive emails (including emails that are subject to statutory retention periods) should be retained and only for as long as required (see the Bar Council's guidance on retention of data).

9. The General Data Protection Regulation ("UK GDPR") requires that you only retain personal data which it is necessary for you to retain in relation to the purposes for which you require the personal data. Emails containing personal data which are no longer required therefore need to be deleted in accordance with your Privacy Notice and Data Retention Policy. Likewise, other emails containing confidential information of clients should be deleted when those emails are no longer required. Careful consideration should be given to the nature of the emails and attachments that are to be retained, and those that are deleted or left to expire from storage.

10. Where some correspondence about a matter is stored electronically and the rest is on paper, barristers and chambers should ensure that none of the material is overlooked if the brief is transferred (perhaps temporarily).

11. Barristers should be aware of the need to provide for the appropriate security of their email correspondence and any attachments, in the same way as they are expected to take reasonable precautions to provide for the security of their computers and any other means of communication they use when dealing with the affairs of a client. Further, email correspondence needs to be backed up at regular intervals.

12. In March 2022, the Information Security Questionnaire for all centralised services provided by Chambers was published on the Bar Council's website, and is an appropriate starting point for considering the security and storage of email correspondence.

13. In May 2024, version 2 of the Questionnaire was published to include questions regarding disaster recovery, business continuity and incident management, in addition to data and device management. Email use and access is highly relevant to these new areas contained within the Questionnaire (v.2); therefore, reviewing policies and procedures is advised.

Unsolicited Bulk Commercial Email (Spam)

14. Spam and bulk mail is an irritant that adversely affects email systems and often makes a negative impression on professional clients and the general public.

15. Barristers or chambers who are considering email marketing campaigns should familiarise themselves with the requirements of the DPA, the UK GDPR, the Electronic Commerce (EC Directive) Regulations 2002, SI 2002 No.2013, the Distance Selling Directive (Directive 97/7/EC) and the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR) (which provides that you must not send marketing emails or text messages to individuals without specific consent, although there is a limited exception for your previous clients, called the 'soft opt-in'), the Regulations concerning comparative and misleading advertising (The Consumer Protection from Unfair Trading Regulations (SI 2008/1277), the Consumer Rights Act 2015, and The Business Protection from Misleading Marketing Regulations 2008 (SI 2008/1276), as amended by the Business Protection from Misleading Marketing (Amendment) Regulations 2013/2701, which forbids misleading advertising.

16. Guidance on the PECR (which has special rules for unsolicited direct marketing by email) 'Direct Marketing' (v2.2) is available on the Information Commissioner's website. https://ico.org.uk/.

Programs that track emails and attachments

17. Software programs have been developed that enable the person sending an email to be informed automatically (i) when the recipient receives and opens the email, (ii) to inform you to whom the email is forwarded, and (iii) to track whether any attachments are opened (by whom and at what time/date).

18. By using such software, you may compromise client confidentiality and professional privilege. It may also be contrary to the UK GDPR.

19. Further information can be found via the following links:

- Chad Gillies, 'Email Tracking: Is It Ethical? Is It Even Legal?', ABA/BNA Lawyers' Manual on Professional Conduct, Current Reports, 33 Law. Man. Prof. Conduct 21, 1/11/17
- New York State Bar Association Committee on Professional Ethics Opinion #749 - 12/14/2001
- Alaska Bar Association, Ethics Opinion 2016-1

20. It is desirable to avoid using a chambers email address for personal emails and as a login for websites relating to non-professional activities (such as social media).

The Data Protection Act 2018 ("the DPA") and the General Data Protection Regulation ("UK GDPR")

21. Self-employed barristers are data controllers, and are therefore required by the DPA to pay a fee to the Information Commissioner ("ICO"). The ICO maintains a public register of data controllers and processors who pay a fee.

22. The UK GDPR contains more stringent obligations in relation to the processing of personal data than existed under the 1998 Act. Guidance from the ICO on the UK GDPR is available here, and the Bar Council's guide is available here.

23. Emails containing personal data must be processed in accordance with the UK GDPR, including the principles set out in Art.5:

> *Personal data shall be:*
>
> *(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');*
>
> *(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; … ('purpose limitation');*

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; … ('storage limitation');

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

24. Personal data may only be processed if at least one of the conditions set out in the UK GDPR and the DPA is satisfied.

25. Data subjects may be entitled to request and receive a copy of the personal data held on them by data controllers. This may include personal data contained in emails and may include 'deleted' emails.

26. Given that barristers and chambers will already have a privacy policy in place, it is likely that in most cases this will govern the UK GDPR-compliant use, processing and retention of personal data contained within emails and attachments.

27. Special rules apply to personal data falling within "Special categories" (formerly known as "sensitive personal data"), personal data relating to criminal offences, disclosures made in connection with legal proceedings, and to processing for the purpose of obtaining legal advice or for establishing, exercising or defending legal rights.

28. Severe penalties may be imposed by the ICO for failure to comply with the UK GDPR.

29. The ICO has provided easy to follow guidance on Emails and Security which tells organisations what *"must"*, *"should"* and *"could"* be done (Link: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/security/email-and-security/)

Threats to email security

30. As it is often said, the internet is inherently insecure. Bear in mind that messages may pass through the hands of unregulated service providers; the networks

used by the internet are vulnerable to hacking; and governments can undertake interception on a substantial scale. Email can bring viruses, malicious software and ransomware into chambers' systems. Viruses and malicious software may damage systems; interfere with service to clients; distribute confidential information, or allow unauthorised access to it. Ransomware can encrypt a single device or an entire system, locking everyone out of their files. The perpetrator invariably demands payment (usually in a crypto currency) to provide the key to de-crypt the files or system. However, there is no guarantee that payment will lead to the release of the files.

31. The most likely cause of confidential information in an email being received by an unintended recipient is human error: the sender typing in the wrong email address. Less likely, but still technically possible, is the risk of an email message being accidentally misrouted to the wrong recipient or intercepted intentionally by a third party. Barristers and chambers that carelessly expose sensitive communications to these risks may be liable for breach of professional conduct rules or exposed to civil claims for breach of client confidentiality, and a large fine may be imposed by the ICO.

32. External threats include the activities of hackers who seek to obtain access to systems and networks, attacks on websites, appropriating content from your website, attacks on your image or brand by defacing or altering the website, denial of service attacks, and phishing – the method used to obtain sensitive information such as usernames, passwords, and credit card details by masquerading as a trustworthy person in an email. Successful and serious external breach of Chambers' system security or interception of emails by a third party is an increasing risk and the number of attacks continues to rise. The vulnerability of systems with 'always-on' unsecured broadband connection to the internet is significant. It typically takes less than an hour from first connection for an 'always-on' system to be attacked. At a minimum, such systems should be protected with properly configured firewalls.

33. Internal threats should not be ignored. A disgruntled former member of staff may deliberately abuse his or her access. Systems administrators and other IT staff employed by, or contracted to, a chambers are in a particularly privileged position as regards access to confidential material. They should all be carefully vetted before being taken on. Encryption of sensitive documents may be necessary to prevent technical support staff obtaining access to them. Ensure that technical staff do not have an unauthorised back-door route to obtain access (by logging on as a user for example).

34. The Information Security Questionnaire, version 2, now has specific standalone questions in relation to phishing, vulnerabilities and penetration testing. There is also a voluntary cyber and information security affirmation. Answering the Questionnaire to meet the security affirmation is a good start to ensure email security.

Security measures for chambers

35. Chambers should maintain up-to-date technical precautions against such risks, ensure that users are alert to the importance of complying with associated procedures and are encouraged to consider the Information Security Questionnaire for all centralised services provided by Chambers.

36. Chambers are recommended to adopt systems that:

36.1. Provide the facility for retrieving (and automatically decrypting) encrypted incoming mail; and

36.2. If the client requires you to encrypt emails, then you or your chambers must have the capacity to do that.

37. Chambers should keep private cryptographic keys securely under their own control and have a key management policy. They should not rely on the use of encrypted communication links for which service providers control the cryptographic keys. Chambers should be aware that encryption software using strong cryptography is widely available.

38. Where barristers or chambers are not prepared to accept instructions by email, this should be made clear. In addition, should chambers not accept initial instructions by email, it is for each member to determine whether or not to receive further instructions by this method.

39. In any event, it is important that chambers has a written email policy; it will help to ensure the proper management and supervision of chambers, including compliance with the BSB Handbook (Rule C39) and statutory requirements (including UK GDPR).

40. Measures that may be taken in order to manage the security risks include conducting regular inspections of employee email logs for breaches of security, the logging of access to the private areas of chambers' networks and communicating chambers' policies to all members of staff by way of an IT usage policy.

Automated email warnings for confidential and legally privileged correspondence

41. Barristers' advice, opinions and professional correspondence are generally confidential and may attract legal professional privilege. Chambers and individual barristers should adopt confidentiality warnings for email.

42. While automated confidentiality warnings are unlikely to impose any legally binding duty on an unintended recipient, many recipients may be expected to heed them, and the warnings may therefore help prevent a mistake from causing loss.

43. The below is a typical form of automated warning:

> "Information in or attached to this message is confidential and may be legally privileged. If you are not the intended recipient, please notify the sender, and please delete the message from your system immediately."

44. Email servers can be configured to add a warning to all outgoing email. A warning could form part of a signature block. Automatic inclusion of a warning is recommended. Alternatively, barristers and chambers could prepare a template for use as and when needed. The signature can also contain a link to the barrister's Privacy Notice.

Forwarding emails from chambers systems to personal email accounts

45. It is possible to forward emails from the chambers system to a different email account, thus enabling a barrister to collect their emails outside the chambers domain. Should a barrister have their emails forwarded in this way, they should be aware of the security implications that arise. For example, unless the barrister is confident that their personal email hosting service complies with data protection rules, forwarding emails to a personal account may breach the provisions of the UK GDPR as it may result in personal data being transferred outside the EEA (see the Bar Council's document on data security).

IT Usage Policy

46. Implementing and enforcing an IT usage policy which is drafted to be consistent with industry best practice, will also help to mitigate the risk of successful claims being brought against chambers for breaches of confidence committed by members of their staff.

47. Chambers should ensure that all relevant devices including laptops, smartphones, tablets and home computers used for business-related work are brought within the scope of their IT and email security policies. Chambers should have regard to the guidance on Information Security provided by the Bar Council, which addresses these matters in more depth.

CJSM

If you are a criminal practitioner, and communicate regularly with any of the following Criminal Justice Organisations (CJOs) – Police, Probation, CPS, Crown Courts, Magistrates' Courts, Prisons and the Youth Justice Board – and Criminal Justice IT (CJIT); or you communicate with private defence solicitors or the Criminal Defence Service by email, you probably already use the CJSM email which allows secure and encrypted communication between all of these organisations. For further

information log on to the CJSM website for specific enquiries. Alternatively, the CJSM HelpDesk number is 0870 010 8535/020 7604 5598.

Important Notice

This document has been prepared by the Bar Council to assist barristers on matters of IT. **It is not "guidance" for the purposes of the BSB Handbook I6.4, and neither the BSB nor bodies regulating information security nor the Legal Ombudsman is bound by any views or advice expressed in it.** It does not comprise - and cannot be relied on as giving - legal advice. It has been prepared in good faith, but neither the Bar Council nor any of the individuals responsible for or involved in its preparation accept any responsibility or liability for anything done in reliance on it. For fuller information as to the status and effect of this document, please see here.

Annex A: Sample Chambers Email and Social Media Policy

[Name of Chambers]

Policy on the use of Chambers' IT Systems

Introduction

The purpose of this policy is to provide a short guide to the rules that chambers require to be observed by users of its Information Technology (IT) systems. By IT systems, we mean telephones, computers including (without limitation) PDAs, smartphones and other telecommunications equipment.

This policy is intended to contain guidance on the conduct of members of chambers and of chambers' clerks and staff. All are expected to exercise professional judgement at all times.

Comments on the policy are welcome; they, together with any requests for clarification, should be addressed to [insert position].

Security

All members of chambers and staff are responsible for the security of the device(s) allocated to them, and must not allow them to be used by another person unless permitted by this policy.

Passwords are unique to each user, and must not be made available to any other member of staff unless authorised by [insert position].

Inappropriate Use of Chambers' Equipment and IT Systems

Access is granted to the internet, and to other chambers' systems, only for legitimate business purposes. Incidental personal use is permissible provided it is in full compliance with chambers' rules, policies and procedures, such as this policy and its Equal Opportunities Policy, its Anti-Harassment Policy, its disciplinary rules, [and insert any other relevant policies].

Under no circumstances should chambers' equipment or IT systems be used to send, receive, browse, download or store material which may be illegal, offensive or cause embarrassment to others. This includes (without limitation) the use of systems to send, receive, obtain access to, download or store pornographic material and material which is racially or sexually offensive.

The observations made below refer to your general use of the internet, including the use of social media to post comments.

Personal Use of Chambers' Facilities

The minimal use of chambers' IT facilities by chambers' staff to send personal email or to browse the internet is acceptable provided that:

i. The usage is minimal and takes place substantially out of normal working hours;

ii. Whenever it takes place, the usage does not interfere with client or office commitments;

iii. The usage does not commit chambers to any marginal costs (at present the marginal cost of sending or browsing the web may be taken to be zero); and

iv. The usage complies with chambers' policies.

This policy on personal use is designed to be liberal, but its continuance is dependent upon its not being abused or overused and may be withdrawn or amended.

Use of a chambers email address for personal emails and as a login for websites relating to non-professional activities (such as social media) should be avoided.

Emails Generally

Take care in what you say in email messages. Improper statements can give rise to personal or client liability. Work on the assumption that email messages may be read by others, and do not include in your emails anything which would offend or embarrass any such reader, or would embarrass chambers if it found its way to the public domain.

Specifically:

i. Never send abusive, obscene, sexist, racist, harassing or defamatory messages. If you receive such a message, do not forward it to anyone. Report it to [insert position].

ii. If a recipient asks you to stop sending them personal messages then always immediately stop. Please take note of chambers' Anti-Harassment Policy.

iii. If your system permits email name changing, do not send messages from another member of staff's computer under a name other than your own name (although clerks are permitted to send emails in their own name on behalf of any members of chambers if instructed to do so by him or her provided that they use the email tool which automatically states at the top of the email that it is sent on behalf of the relevant barrister).

iv. Do not send confidential messages by email without the approval of the client or the instructing solicitor.

v. Never open an email attachment from an unexpected or untrustworthy source or if, for any reason, it appears 'suspicious' (for example, if it ends in .exe or .pif). Viruses and ransomware are propagated by email. If you suspect that a virus has infected your computer inform [insert position].

vi. Email messages can be documents which are disclosed in legal or costs proceedings if relevant to the issues unless protected by privilege. Therefore, always exercise the same caution in what you say in emails as you would in more formal correspondence.

vii. Never send or forward private emails at work which you would not want a third party to read.

viii. Do not create email congestion by sending trivial messages or unnecessarily copying emails to those who do not have a real need to have them.

ix. Do not send or forward "chain-mail" emails as they have a propensity to over-load the system.

x. Do not advertise by email except in accordance with the relevant regulations.

xi. Always remember that text, music and other content on the internet are copyright works. Never download or email such content to others unless you are certain that the owner of such works allows this.

xii. If sending important information or work by email, always obtain confirmation of receipt (either by requesting a reply to your email, or by following up with a telephone call). Do not use programs that notify you automatically when the recipient receives and opens the email, to whom the email is forwarded or/and if the program tracks whether any attachments are opened (by whom and at what time/date).

xiii. Never agree to terms or enter into contractual commitments or make representations by email without having obtained proper authority. When you type your name at the end of an email, this is one form of electronic signature, and the act is just as much a signature as if you had signed it manually.

xiv. Chambers reserves the right, on notice, to monitor staff emails to ensure compliance with this policy and the requirements of the law, the BSB Handbook and data protection.

External emails

Never send strictly confidential messages via the internet, or by other means of external communication which are known not to be secure. If you send advices or opinions by email, you are responsible if they are incorrectly addressed or delivered to the wrong mailbox.

If requested to forward information over the internet, or you send work by email, make sure that your instructing solicitor knows that it is not totally secure and is willing to accept that risk.

The internet

The component parts of web pages are routinely stored on the "viewing computer" in order to improve access times should the site be re-visited. This is called "caching" web pages. It is therefore highly likely that images etc. (whether in fact viewed or not) will remain on the computer used to obtain access to the site. If the images are inappropriate than this could lead to embarrassment to chambers. Further, it should be noted that the cached items may remain on the system for a considerable period of time after the item is placed there.

It should also be pointed out that if you visit a site, you are likely to receive cookies which may enable the site owner to work out who has visited. These cookies can also be used to discover the pages that the viewer has visited prior to the site owner's page or visits later. Data from the website will also be stored in a cache on the user's device.

If the website is an inappropriate one, the record of the visit to the website could embarrass chambers. If you obtain access to, download, store or forward inappropriate material others might be offended.

In some cases you may be committing a criminal offence if, for example, the material is pornographic in nature.

An additional problem is where somebody adds "rogue code" in web pages that can be used to infect the viewing computer. Such code is more usually to be found in the less reputable sites on the internet (but highly respectable websites have had this code added without the knowledge of the owner) which will also be those more likely to cause embarrassment to chambers if it is discovered that they have been viewed.

"Phishing" is the process by which criminals try to make use of emails or telephones calls to deceive users into revealing confidential information, including usernames and passwords. Such fraudulent emails typically include links to false websites pretending to be the websites of legitimate institutions or businesses. The inclusion of a recognisable logo, or the use an email address, are by themselves insufficient to prove that a given email request is genuine. Always be cautious about the veracity of

an emailed request for confidential information or an email which includes a direct link to a website which then asks for such details, or to sign in.

For example, a link sent might ask a user to reset a password or update account contact details. An email might simply ask you to log on to a site you ordinarily use using your confidential password and email address. Any information put into a false web page would then fall into the hands of criminals who could then use, sell on or circulate those details. Often information which is non revocable, such as dates of birth or family names, can then be used to try to obtain access to bank accounts and other secure services well after the successful phishing attempt.

For any significant website, such as a banking website, type the full advertised web address for the institution, rather than trust a link sent by email. Do not rely on a search engine to obtain access to an important financial site. If in doubt, obtain access to the business, service or institution through your normal bookmark or phone application, rather than just through a search engine or by clicking on a link in an incoming email.

Never send a payment to a bank account identified in an email unless you have checked with the payee by telephone that the bank account details are correct, or you have previously made a payment to that bank account.

You should cross-refer to chambers' Anti-Harassment Policy. For these reasons, you should adhere to the following policies:

i. See the rules on personal use referred to above.

ii. Do not obtain access from chambers' system any web page which, on the widest meaning of those terms, could be regarded as illegal, offensive, in bad taste or immoral. This definition is intended to be interpreted very widely: content may be perfectly legal in the UK yet in sufficient bad taste to fall within this prohibition. Sometimes the content may be against the law. As a general rule, if any person within chambers' (whether intended to view the page or not) might be offended by the contents of a page, or if the fact that chambers' software has obtained access to the page might embarrass chambers if made public, then it may not be viewed.

iii. The same rule applies to any files (whether documents, images or other) downloaded from the web.

Security – Home Software

Security issues encompass the need to ensure that chambers is protected both against misuse of others' copyright material, for example by loading onto office machines programs that are not properly licensed; and against computer viruses, for example

by loading onto chambers machines programs or files which have not been properly virus checked. Accordingly, you may not load onto office machines any software not provided by chambers without the permission of [insert position].

You should familiarise yourself with relevant Bar Council documents which can be found on the Ethics and Practice Hub.

Review

This policy will be reviewed annually.

Important Notice

This document has been prepared by the Bar Council to assist barristers on matters of IT. **It is not "guidance" for the purposes of the BSB Handbook I6.4, and neither the BSB nor bodies regulating information security nor the Legal Ombudsman is bound by any views or advice expressed in it**. It does not comprise - and cannot be relied on as giving - legal advice. It has been prepared in good faith, but neither the Bar Council nor any of the individuals responsible for or involved in its preparation accept any responsibility or liability for anything done in reliance on it. For fuller information as to the status and effect of this document, please see website here.