POLICY—INTERNET, EMAIL AND COMMUNICATIONS

You are required to read this policy because it gives important information about:

- the Institute of Barrister's Clerks (the IBC) rules on the use of internet, email, telephone and other communications systems at work, including in relation to confidentiality, security and personal use;
- how the IBC monitors the use of those systems;
- your rights and obligations in relation to data protection;
- the consequences of failure to comply with this policy; and
- review and training.

Once you have read and understood this policy, please confirm you that have done so by signing and returning the attached copy to [insert name and/or position].

1 Introduction

1.1 The IBC recognises that the use of email and internet can save time and expense, and is an important part of the way we work. However, it brings with it certain risks, some of which may involve potential legal and financial liabilities for both the IBC and the individual, e.g.:

1.1.1 inadvertently entering into contracts or commitments on behalf of the IBC;
1.1.2 introducing viruses into the IBC's systems;
1.1.3 breaching copyright or licensing rights;
1.1.4 breaching data protection rights;
1.1.5 breaching confidentiality and security;
1.1.6 defamation; and/or
1.1.7 bullying, harassment and discriminatory conduct.

1.2 This policy aims to guard against those risks. It is therefore important that all staff read the policy carefully and ensure that they use the internet, email and other communication systems in accordance with it. If you are unsure whether something you are about to do complies with this policy, you should seek advice from your line manager.

1.3 This policy also explains when the IBC monitors the use of email and the internet and the action the IBC will take if the terms of this policy are breached.

1.4 References in this policy to 'email' apply equally to other electronic communications, messaging tools and posts.

1.5 The IBC expects its computer and communications systems and equipment to be used in an effective and professional manner, and encourages all staff to develop the necessary skills to achieve this. These systems and equipment are provided by the IBC for the purpose of the business, and to assist staff in carrying out their

duties effectively. It is the responsibility of all staff to ensure that these systems and equipment are used for proper business purposes and in a manner that does not compromise the IBC or its staff in any way.

1.6 The IBC's principles of integrity, professionalism and ethical business practice must be applied equally to email and internet use. All staff should consider how their reputation and that of the IBC might be affected by how they communicate and conduct themselves online.

1.7 [Insert name and/or position] is responsible for the monitoring and implementation of this policy. Any questions about the content or application of this policy or other comments should be referred to [insert name and/or position].

2 Scope

2.1 This policy applies to all staff, including employees, workers, temporary and agency workers, interns, volunteers and apprentices, and to consultants and other contractors who have access to IBC computer and other communications systems. It also applies to personal use of the IBC's systems and equipment in any way that reasonably allows others to identify any individual as associated with the IBC.

2.2 This policy applies to the use of IBC email, telephone and internet systems both in the workplace and from outside it, e.g., via remote access. It also applies to the use of an IBC laptop, tablet, mobile phone, smartphone or personal digital assistant (PDA).

2.3 All staff must be familiar with this policy and comply with its terms.

2.4 Staff should also refer to the IBC's data protection policy and data protection privacy notice and, where appropriate, to its other relevant policies.

2.5 [Insert name and/or position] is responsible for this policy.

2.6 We will review and update this policy in accordance with changes in technology and the law, and current business practice. It does not form part of any employee's contract of employment and we may amend, update or supplement it from time to time. We will circulate any new or modified policy to staff before it is adopted.

3 Use of the IBC's Computer Systems

3.1 Staff may use the IBC's computer systems (including equipment) for authorised purposes only, i.e. for the purposes of the IBC's business or in accordance with paragraphs [6, 8 and 11] (permitted personal use). If you wish to use the IBC's

Commented [JUD1]: Paragraph 6 = Emails – Personal Use
Paragraph 8 = Telephones – Personal Use
Paragraph 11 = Internet – Personal Use

If you choose not to include these paragraphs, this will require updating accordingly.

systems or equipment for another purpose, you must obtain express permission from [Insert name and/or position] before doing so.

3.2 Use of the IBC's systems for commercial purposes other than those of the IBC's business is strictly prohibited.

3.3 To reduce the risk to the IBC's systems or network of virus infections, hacking and other unauthorised access attempts, you may only access the IBC's systems or network as follows:

3.3.1 from your workplace or other IBC premises, using authorised equipment only;
3.3.2 remotely, via broadband, dial up, etc using authorised equipment via secure means, e.g., VPN software only; or
3.3.3 remotely, using unauthorised equipment, e.g., your home computer or an internet café terminal, via [Citrix **OR** [insert other desktop virtualisation system]] and VPN only.

3.4 The IBC licenses software from a number of sources. The IBC does not own that software and must comply with any restrictions or limitations on use, in accordance with its licence agreements. All staff must adhere to the provisions of any software licence agreements to which the IBC is party.

3.5 Staff must not use any software owned or licensed by the IBC for any purpose other than those of the IBC's business without express permission from [Insert name and/or position] or as otherwise permitted by the terms of this policy.

3.6 Staff must not copy, download or install any software without first obtaining express permission from [Insert name and/or position].

4 Email Use—General

4.1 All communications, including email, should reflect the highest professional standards at all times. In particular, all staff must:

4.1.1 keep messages brief and to the point;
4.1.2 check emails carefully before sending, including spelling and grammar;
4.1.3 ensure that all emails sent from the IBC include [the current disclaimer wording **OR** the following wording: [insert disclaimer wording, *e.g. This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed ('intended recipient'). Accordingly, the dissemination, distribution, copying or other use of this email or any of its content by any person other than the intended recipient may constitute a breach of civil or criminal law and is strictly prohibited. If you are not the intended recipient, please notify our system manager by telephoning [insert number*].]];

4.1.4 ensure that an appropriate heading is inserted in the subject field; and

4.1.5 check the recipient(s) before pressing the send button—not only can it be embarrassing if a message is sent to the wrong person, it can also result in the unintentional disclosure of confidential information about the IBC, a client/customer or other third parties.

4.2 Staff must not send messages from another person's email address (unless authorised in the proper performance of their duties), or under an assumed name.

4.3 Staff must not send or post messages or material that are offensive, obscene, defamatory or otherwise inappropriate in the work environment. This includes, but is not limited to messages that:

4.3.1 are inconsistent with the IBC's [Equality Policy] and/or [Harassment and Bullying Policy];

4.3.2 criticise the IBC's competitors or their staff;

4.3.3 suggest that there are quality problems with goods or services of suppliers, clients or customers; or

4.3.4 state that anyone is incompetent.

4.4 Staff must not send or post any message or material which could be regarded by the recipient or any other person as personal, potentially offensive or frivolous.

4.5 Equally, if you receive a message that is offensive, obscene, defamatory or inappropriate in the work environment, you must delete it immediately and not forward it to any internal or external recipient, other than internally to [Insert name and/or position] in order to report a breach of this or another IBC policy.

4.6 Staff should not send or post anything in an email that they would not be comfortable writing (or someone else reading) in a letter. Emails leave a retrievable record and, even when deleted, can be recovered from the IBC's back-up system or an individual's computer. They are admissible as evidence in legal proceedings and have been used successfully in libel and discrimination cases, and they can also be reviewed by regulators.

4.7 Staff must not create congestion on the IBC's systems or network by sending trivial messages, by unnecessary copying or forwarding of messages to recipients who do not need to receive them, or by sending or forwarding chain mail, junk mail, cartoons, jokes or gossip.

4.8 Staff must use a professional email address for sending and receiving work-related emails and must not use their own personal email accounts to send or receive emails for the purposes of the IBC's business. Staff must not send (inside or outside work) any message in the IBC's name unless it is for an authorised, work-related purpose.

4.9 Staff must not send unsolicited commercial emails to persons with whom the individual does not have a prior relationship without the express permission of the relevant manager.

4.10 Emails must not use the IBC's logos or other branding material without the approval of [Insert name and/or position].

4.11 Emails must not provide references, recommendations or endorsements for any third party, unless expressly authorised by [Insert name and/or position].

4.12 [[Emails containing personal data or special categories of personal data may be retained only in accordance with the IBC's [records retention policy].] [Client **OR** Customer]-related emails should be [printed and filed within 48 hours of receipt **AND/OR** attached to the IBC's document management system within 48 hours of receipt]. Emails will generally be stored on the IBC's server for [insert period, e.g., 12 weeks], after which they will be permanently deleted. If an individual needs to keep any emails beyond this date that are not [client **OR** customer]-related, these should be stored [insert place, e.g., personal folders].]

4.13 Staff must be vigilant when using the IBC's email system. Computer viruses are often sent by email and can cause significant damage to the IBC's information systems or network. Be particularly cautious in relation to unsolicited emails from unknown sources.

4.14 If any individual suspects that an email may contain a virus, they should not reply to it, open any attachments to it or click on any links in it and must contact [Insert name and/or position] immediately for advice.

5 Emails—Confidentiality

5.1 Staff should not assume that emails sent or received internally or externally are private and confidential, even if marked as such. Email is not a secure means of communication and third parties may be able to access or alter messages that have been sent or received. Do not send any information in an email which you would not be happy being publicly available. Matters of a sensitive or personal nature should not be transmitted by email unless absolutely unavoidable and if so, should be clearly marked in the message header as highly confidential. The confidentiality of internal communications can only be ensured if they are [sent by internal post, **AND/OR** delivered personally by hand **AND/OR** included in a password-protected or encrypted online document].

5.2 Emails should be treated as non-confidential. Anything sent through the internet passes through a number of different computer systems, all with different levels of security. The confidentiality of messages may be compromised at any point along the way unless the messages are properly encrypted.

5.3 Staff should refer to [their contract **AND/OR** the Staff Handbook] for details of the types of information that the IBC regards as confidential and which should be treated with particular care.

5.4 Lists of contacts compiled by staff during the course of their employment and stored on the IBC's email application, information manager and/or other IBC database(s) (irrespective of how they are accessed) belong to the IBC. Such lists may not be copied or removed by staff for use outside their employment or after their employment ends.

6 Emails—Personal Use

6.1 [Although the email system is primarily for business use, the organisation understands that staff may occasionally need to send or receive personal emails while at work.]

6.2 The sending of personal emails using the work email address is [not permitted **OR** therefore permitted. When sending personal emails using the work email address, employees should show the same care as when sending work-related emails].

6.3 [Reasonable personal use of the IBC's systems or network to send personal email is [also] permitted, provided that it does not interfere with the performance of any individual's duties and the terms of this policy are strictly adhered to. We reserve the right, at our absolute discretion, to withdraw this privilege at any time and/or to restrict access for personal use.

OR

The IBC does not permit access to web-based personal email applications such as Hotmail, Yahoo!, Outlook.com or gmail on its systems or network at any time, due to the additional security risks to the IBC's systems or network.]

6.4 [Personal use must meet these conditions (in addition to those set out elsewhere in this policy):

6.4.1 personal use must be minimal (both in terms of time spent and frequency) and reasonable and must take place [exclusively **OR** mainly] outside normal working hours, i.e., during lunch or other breaks, or before and after work;

6.4.2 [personal emails must be labelled 'Personal' in the subject header[and in the sensitivity settings];]

6.4.3 personal use must not affect the job performance of any member of staff or otherwise interfere with the IBC's business; and

6.4.4 it must not commit the IBC to any marginal costs.]

7 Emails—Monitoring

7.1 The IBC may monitor the email [and instant messaging] systems or network in the workplace for the following reasons:

7.1.1 to determine whether they are communications relevant to the carrying on of the IBC's relevant activities;

7.1.2 if the individual is absent from work, to check communications for business calls to ensure the smooth running of the business;

7.1.3 to record transactions;

7.1.4 where the IBC suspects that the individual is sending or receiving messages that are:

(a) detrimental to the IBC;
(b) in breach of the individual's contract, or this policy;
(c) in breach of data protection rights;

7.1.5 to monitor staff conduct;

7.1.6 to investigate complaints, grievances or criminal offences.

7.2 When monitoring incoming or outgoing emails, the IBC will, unless exceptional circumstances apply:

7.2.1 look at the sender or recipient of the email and the subject heading only; and

7.2.2 avoid opening emails marked 'Private' or 'Personal'.

7.3 [The IBC uses a data loss prevention (DLP) tool to monitor outgoing email traffic, looking at the intended recipient of the email and the subject heading only. If a potential data breach is identified, where possible the sender will be warned before transmission and given the option of cancelling the transmission.

OR

The IBC does not, as a matter of policy routinely monitor employees' use of the internet or the content of email messages sent or received. However, the IBC has a right to protect the security of its systems or network, check that use of the system is legitimate, investigate suspected wrongful acts and otherwise comply with legal obligations imposed upon it. To achieve these objectives, the IBC carries out random spot checks on the system which may include accessing individual email messages or checking on specific internet sites searched for

and/or accessed by individuals. [Insert any further statement explaining the purposes for which any monitoring is conducted, the extent of the monitoring and the means used for monitoring.]]

7.4 The IBC will only intercept (i.e., open) outgoing or incoming emails, received emails, sent emails and draft emails where relevant to the carrying on of the IBC's business and where necessary:

7.4.1 to determine whether the message is relevant to the carrying on of the IBC's business;

7.4.2 to establish the existence of facts;

7.4.3 to check whether regulatory or self-regulatory practices or procedures to which the IBC or its staff are subject have been complied with, i.e., to detect unauthorised use of the system;

7.4.4 to check whether staff using the system in the course of their duties are achieving the standards required of them;

7.4.5 for the purpose of investigating or detecting the unauthorised use of the system;

7.4.6 for the purpose of preventing or detecting crime; or

7.4.7 for the effective operation of the telecommunication system.

7.5 The content of emails will be examined only in exceptional circumstances, initially by [Insert name and/or position]. The information obtained through monitoring may be shared internally[, with members of the HR department, your line manager [insert others e.g., managers in the business area in which the employee works], if access to the information is necessary for the performance of their roles. Information will usually only be shared in this way] where [Insert name and/or position] believes there may have been a breach of the individual's contract or this Policy.

8 Telephones—Personal Use

8.1 [Although the telephone system is primarily for business use, the IBC understands that staff may occasionally need to make or receive personal telephone calls while at work.] The making or receiving of personal telephone calls while at work using [the IBC's telephone system **AND/OR** your personal mobile phone] is [not **OR** therefore] permitted.

8.2 [Personal use must meet these conditions (in addition to those set out elsewhere in this policy):

8.2.1 personal use must be minimal (both in terms of time spent and frequency) and reasonable and must take place [exclusively **OR** mainly] outside normal working hours, i.e., during lunch or other breaks, or before and after work;

8.2.2 it must not affect the job performance of any member of staff or otherwise interfere with the IBC's business;

8.2.3 it must not commit the IBC to any marginal costs; and

8.2.4 you may not use the telephone during working hours to perform work for yourself or another employer, or to look for work; or

8.2.5 you may not communicate confidential information other than in the course of your duties, or act in a way that is detrimental to the IBC.]

8.3 [Charges for personal telephone calls made using the IBC's telephone system over a certain amount each month must be reimbursed to the IBC in accordance with the IBC's [insert details, e.g., expenses policy].]

8.4 [The IBC's telephone system may not be used for premium rate or international calls[unless expressly authorised by the individual's manager].]

9 [Telephones—Monitoring

9.1 The IBC may monitor the use of its telephone system, and IBC mobile phones (including smartphones) for the following reasons:

9.1.1 if the individual is absent from work, to check communications (including the individual's voicemail) for business calls to ensure the smooth running of the business;

9.1.2 to record transactions;

9.1.3 where the IBC suspects that the individual is acting in a way that is:

(a) detrimental to the IBC;
(b) in breach of the individual's contract, or this Policy;
(c) in breach of data protection rights;

9.1.4 to monitor staff conduct;

9.1.5 to investigate complaints, grievances or criminal offences.

9.2 When monitoring telephones, the IBC will, unless exceptional circumstances apply, look at the numbers from which calls are received and the numbers dialled and the duration and frequency of calls.

9.3 The IBC will only intercept (i.e., listen to) telephone calls or saved messages where relevant to the carrying on of the IBC's business and where necessary:

9.3.1 to determine whether the message is in fact relevant to the carrying on of the IBC's business;

9.3.2 to establish the existence of facts;

9.3.3 to check whether regulatory or self-regulatory practices or procedures to which the IBC or its staff are subject have been complied with, i.e., to detect unauthorised use of the system;

9.3.4 to check whether staff using the system in the course of their duties are achieving the standards required of them;

9.3.5 for the purpose of investigating or detecting the unauthorised use of the system;

9.3.6 for the purpose of preventing or detecting crime; or

9.3.7 for the effective operation of the telecommunication system.

9.4 Telephone calls will be intercepted only in exceptional circumstances, initially by [Insert name and/or position]. The information obtained through monitoring may be shared internally[, with members of the HR department, your line manager [insert others e.g., managers in the business area in which the employee works], if access to the information is necessary for the performance of their roles. Information will usually only be shared in this way] where [Insert name and/or position] believes there may have been a breach of the individual's contract or this Policy.]

10 Internet—General

10.1 Access to the internet during working time is [strictly limited to **OR** primarily for] matters relating to your work duties and employment. [Reasonable, limited personal use of the internet is permitted in accordance with paragraph 11.]

Commented [JUD2]: Paragraph 11 = Internet – Personal Use

If you choose not to include this paragraph, this wording should be deleted.

10.2 Any unauthorised use of the internet is strictly prohibited. Unauthorised use includes (but is not limited to):

10.2.1 creating, viewing or accessing any webpage, or posting, transmitting or downloading any image, file or other information that is unrelated to your

employment and, in particular, which could be regarded as pornographic, illegal, criminal, offensive, obscene, in bad taste or immoral and/or which is liable to cause embarrassment to the IBC or to our clients/customers and/or suppliers;

10.2.2 engaging in computer hacking and/or other related activities; and

10.2.3 attempting to disable or compromise security of information contained on the IBC's systems or network or those of a third party.

10.3 Staff are reminded that such activity may also constitute a criminal offence.

10.4 Posts placed on the internet may display the IBC's address. For this reason, staff should make certain before posting information that the information reflects the standards and policies of the IBC. Under no circumstances should information of a confidential or sensitive nature be placed on the internet. Staff must not use the IBC's name in any internet posting (inside or outside work) unless it is for a work-related purpose.

10.5 Information posted or viewed on the internet may constitute published material. Therefore, reproduction of information posted or otherwise available over the internet may be done only by express permission from the copyright holder. Staff must not act in such a way as to breach copyright or the licensing conditions of any internet site or computer program.

10.6 [Staff must not commit the IBC to any form of contract through the internet [without the express permission of their manager].]

10.7 Subscriptions to news groups, mailing lists and social networking websites are permitted only when the subscription is for a work-related purpose. Any other subscriptions are prohibited.

10.8 The IBC may block or restrict access to any website at its discretion.

11 [Internet—Personal Use

11.1 Reasonable personal use of the IBC's systems or network to browse the internet is allowed provided that it does not interfere with the performance of any individual's duties and the terms of this policy are strictly adhered to. The IBC reserves the right, at its absolute discretion, to withdraw this privilege at any time and/or to restrict access for personal use.

11.2 Personal use must meet these conditions (in addition to those set out elsewhere in this policy):

11.2.1 personal use must be minimal (both in terms of time spent and frequency) and reasonable and [must take place exclusively **OR** should take place mainly] outside normal working hours, i.e., during lunch or other breaks, or before and after work;

11.2.2 personal use must not affect the job performance of any member of staff or otherwise interfere with the IBC's business; and

11.2.3 it must not commit the IBC to any marginal costs.]

12 Internet—Monitoring

12.1 The IBC may monitor internet usage (including searches made, the IP addresses of sites visited, and the duration and frequency of visits) if the IBC suspects that the individual has been using the internet in breach of the individual's contract or this policy, e.g.:

12.1.1 by viewing material that is pornographic, illegal, criminal, offensive, obscene, in bad taste or immoral and/or which is liable to cause embarrassment to the IBC or to its clients/customers;

12.1.2 by spending an excessive amount of time viewing websites that are not work-related.

12.2 Monitoring may include internet usage at the workplace, internet usage outside the workplace during working hours using IBC systems or network and internet usage using hand-held or portable electronic devices.

12.3 Monitoring will normally be conducted by [Insert name and/or position]. The information obtained through monitoring may be shared internally[, with members of the HR department, your line manager [insert others e.g., managers in the business area in which the employee works], if access to the information is necessary for the performance of their roles. Information will usually only be shared in this way] where [Insert name and/or position] believes there may have been a breach of the individual's contract or this Policy.

13 Passwords and Security

13.1 Each individual is personally responsible for the security of all equipment allocated to or used by them. An individual must not allow equipment allocated to that person to be used by any other person other than in accordance with this policy.

13.2 Each individual must use passwords on all IT equipment allocated to them, must keep any password allocated to them confidential and must change their password regularly.

13.3 No individual may use another person's username and/or password to access the IBC's systems or network, nor may any individual allow any other person to use their password(s). If it is anticipated that someone may need access to an individual's confidential files in their absence, that individual should arrange for the files to be copied to a network location that is properly secure where the other person can access them or give the person temporary access to the relevant personal folders.

13.4 All staff must log out of the IBC's system or lock their computer when leaving their desk for any period of time. All staff must log out and shut down their computer at the end of the working day.

14 IBC Systems and Data Security

14.1 [You must not download or install software from external sources without prior authorisation from [insert name and/or position]. **OR** Any files or software downloaded from the internet or brought from home must be virus-checked before use. Staff should not rely on their own computer to virus check any such programs but should refer direct to [insert name and/or position].]

14.2 You must not connect any personal computer, mobile phone, laptop, tablet, USB storage device or other device to the IBC's systems or network without express prior permission from [insert name and/or position]. Any permitted equipment must have up-to-date anti-virus software installed on it and the IBC may inspect such equipment in order to verify this.

14.3 You must not run any '.exe' files, particularly those received via email, unless authorised to do so in advance by [insert name and/or position]. Unauthorised files should be deleted immediately upon receipt without being opened.

14.4 You must not access or attempt to access any password-protected or restricted parts of the IBC's systems or network for which you are not an authorised user.

14.5 You must inform [insert name and/or position] immediately if you suspect your computer may have a virus, and you must not use the computer again until informed it is safe to do so.

14.6 All laptop, tablet, smartphone and mobile phone users should be aware of the additional security risks associated with these items of equipment. All such equipment must be locked away in a secure location if left unattended overnight.

15 Prohibited Use and Breach of this Policy

15.1 The IBC considers this policy to be extremely important. Any breach of the policy will be dealt with under the IBC's [insert details, e.g., Code of conduct and

dismissal and disciplinary procedure]. In certain circumstances, breach of this policy may be considered gross misconduct and may result in immediate termination of employment or engagement without notice or payment in lieu of notice. In addition, or as an alternative, the IBC may withdraw an individual's internet and/or email access.

15.2 Examples of matters that will usually be treated as gross misconduct include (this list is not exhaustive):

15.2.1 unauthorised use of the internet as outlined in paragraph 10.2 above;

15.2.2 creating, transmitting or otherwise publishing any false and defamatory statement about any person or organisation;

15.2.3 creating, viewing, accessing, transmitting or downloading any material which is discriminatory or may cause embarrassment to other individuals, including material which breaches the principles set out in the IBC's [Equality Policy] and/or [Harassment and Bullying policy];

15.2.4 accessing, transmitting or downloading any confidential information about the IBC and/or any of our staff and/or client or customers, except where authorised in the proper performance of your duties;

15.2.5 accessing, transmitting or downloading unauthorised software; and

15.2.6 viewing, accessing, transmitting or downloading any material in breach of copyright.

Commented [JUD3]: Paragraph 10 = Internet – General
Paragraph 10.2 sets out examples of unauthorised use of the internet.

I have read and understood this policy and agree to abide by its terms.

Signed: _____

Name: _____

Date: _____