This template Internet and electronic communications policy sets out a suggested policy for use of the Internet and other electronic communication systems while at work and also when using firm technology outside of work.

It also covers social media

Internet, e-comms and social media policy

***This template is produced in partnership with Lexis®PSL Practice Compliance.***

*Lexis®PSL Practice Compliance is an online service designed to make risk and compliance easier to manage, whatever the size of your firm.   It comes with everything you need to get your compliance house in order and keep it that way, including an unbeatable range of practical guidance, templates, flowcharts, checklists and other time-saving tools.*

*See more at* [*https://www.lexisnexis.com/uk/lexispsl/practicecompliance/home*](https://www.lexisnexis.com/uk/lexispsl/practicecompliance/home)*.*

Internet, e-comms and social media policy

Introduction

1.1 We expect our electronic and computer facilities to be used in an effective and professional manner and encourage all staff to develop the skills necessary to do so. These facilities are provided by the firm at its own expense for its own business purposes to assist staff in carrying out their duties effectively. It is the responsibility of each member of staff to ensure this technology is used for proper business purposes and in a manner that does not compromise the firm or its employees in any way.

1.2 Professional integrity is central to the firm and it must characterise all our dealings. You should think about how your own image or that of your firm may be affected by how you use the internet and other electronic communication systems. The same professional ethical obligations apply to your conduct in online and offline environments.

1.3 This policy applies to the use of firm technology while at work and also when using firm technology from outside work, eg when dialling in from home, using a firm laptop when away on business and when using BlackBerries, smartphones or personal digital assistants. If you have any questions about the application of this policy, please contact [insert job title/department, eg our IT department/IT manager/IT partner/compliance office for legal practice (COLP)].

1.4 This policy applies to [partners OR directors], employees of the firm, workers and other contractors who have access to firm computer systems. It also applies to your personal use of the firm’s equipment and technology in any way that reasonably allows others to identify you as associated with the firm.

1.5 We may occasionally modify this policy to take account of changes in technology, law and best practice. You will be notified in writing of any change.

1.6 The [IT manager OR IT partner OR COLP] is responsible for monitoring and implementing this policy. If you have any questions about the content of this policy or other comments you should contact the [IT manager OR IT partner OR COLP].

1.7 This policy does not form part of any employee's contract of employment. We may amend it at any time and decide to follow a different procedure where we consider it appropriate.

**[[1]](#footnote-1)**

Computer system use

2.1 You may use the firm's computer systems only to the extent you are authorised to do so. You should not use the firm's computer equipment for any purpose that is not connected to the firm's business unless you have express permission to do so or you are making personal use of the system as permitted by this policy.

2.2 If you have access to the firm's network, you must adhere to strict access controls to reduce the risk of virus infections, hacking and other unauthorised access attempts:

2.2.1 only authorised equipment is allowed to connect to the firm's network from any office location

2.2.2 [remote access (via broadband, dial up, etc) is also restricted to authorised equipment and access must only be via secure means, eg VPN software]

2.2.3 the only access allowed to unauthorised equipment, eg internet café terminals, is via [Citrix/other desktop virtualisation system] and VPN

2.3 We license software from a number of sources. We do not own that software and must comply with any restrictions or limitations on use, in accordance with its licence agreements. You must adhere to the provisions of any software license agreements to which the firm is party.

2.4 Unless permitted by this policy, you should not use any software for any purpose outside the business of the firm without express permission of [IT manager OR IT partner OR COLP].

2.5 You should not copy, download or install any software without first obtaining permission from the [IT manager OR IT partner OR COLP].

2.6 We may monitor your use of the firm's computer system in accordance with this policy.

Security

3.1 You must not allow other members of staff to use your password. If you anticipate that someone may need access to one of your personal folder files in your absence, do not share your password. You should instead arrange for the folder to be copied or give shared access to the relevant personal folder.

3.2 Be vigilant when using the firm email system. Computer viruses are often sent by email and can cause significant damage to the firm's IT systems.

3.3 Any files or software downloaded from the internet or brought from home must be virus checked before use. [You must not rely on your own PC to virus check any such programmes but should refer direct to [the IT department OR IT manager OR IT partner].] If you suspect a file may contain a virus, do not open it—contact the [the IT department OR IT manager OR IT partner] immediately.

3.4 You must not run any '.exe' files. These should be deleted immediately on receipt without being opened.

3.5 All laptop and mobile phone users should be aware of the additional security risks associated with these items of equipment. All laptops and mobile phones should be locked away if left unattended overnight.

Email use

4.1 Email, just like any other form of communication, should reflect the highest professional standards at all times. You should:

4.1.1 keep messages brief and to the point

4.1.2 ensure an appropriate heading is inserted in the subject field

4.1.3 ensure the spelling and grammar are carefully checked before sending

4.1.4 double check the recipient before pressing the send button—not only can it be embarrassing if a message is sent to the wrong person, but it can also result in the unintentional disclosure of confidential information about the firm or a client

4.2 You should not transmit anything in an email or fax message that you would not be comfortable writing (or someone else reading) in a letter or a memorandum. Emails leave a retrievable record. Even when you think you have deleted information, it can remain on your computer and on the firm's back-up system. Emails can be recovered as evidence in court proceedings and/or reviewed by regulators. Electronic messages are admissible as evidence in legal proceedings and have been used successfully in libel and discrimination cases.

4.3 You should never assume that internal or external messages are private and confidential, even if marked as such. The internet 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 that 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 OR delivered personally by hand OR included in a password protected online document].

4.4 You should not send unsolicited commercial emails to persons with whom you do not have a prior relationship without the express permission of your manager.

4.5 Although the primary reason for allowing access to email is to help you perform your duties more effectively, reasonable personal use of email will be allowed provided that it does not interfere with the performance of your duties and the terms of this policy are strictly adhered to.

4.6 We may monitor your use of the firm's email facilities in accordance with this policy.

4.7 Emails will be [stored on our server] for [insert period, eg 12 weeks], after which they will be permanently deleted. If you wish to keep any emails beyond this date that are not client-related, you should use your [personal folders]. Any client-related emails should be [printed and filed within 48 hours of receipt OR attached to our document management system with 48 hours of receipt].

4.8 All emails sent from the firm should include the following wording: 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. If you have received this email in error please notify the system manager.

Internet use

5.1 Access to the internet during working time should be limited to matters relating to employment. [However, you may make reasonable personal use of the internet provided it does not interfere with your duties and provided that use is strictly in accordance with this policy].

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

5.2.1 connecting, posting or downloading any information unrelated to your employment and in particular pornographic or other offensive material

5.2.2 engaging in computer hacking and other related activities

5.2.3 attempting to disable or compromise security of information contained on the firm's computers

5.3 You are reminded that such activity may constitute a criminal offence.

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

5.5 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 with express permission from the copyright holder. You must not act in such a way as to breach copyright or the licensing conditions of any internet site or computer programme.

5.6 You must not commit the firm to any form of contract through the internet [ without the express permission of your manager].

5.7 Subscriptions to news groups and mailing lists are permitted only when the subscription is for a work-related purpose.

5.8 We may monitor your use of the internet in accordance with this policy.

Social media

6.1 Social media means media such as blogs, web forums, social networking sites, such as [Twitter, Facebook and Linked In], instant messaging and other publicly available communication and content-sharing systems and sites.

6.2 The firm [[and its staff OR and appointed staff ]] use[s] social media to support and promote our business objectives [as described in our business plan].

6.3 It is important to maintain consistent standards in relation to the firm's use of social media. This policy contains guidelines for engaging in social media. We may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be circulated to staff before being adopted. [We will publish the policy and any supplementary guidelines on our intranet.]**[[2]](#footnote-2)**

6.4 When you post a message using social media you are making a public statement. Your messages will not be private and can be forwarded to third parties without your consent. Once sensitive or confidential information (or offensive or defamatory information) has been posted, it cannot be recovered and this may result in liability both for the firm and also you personally.

6.5 All use of social media on behalf of the firm must be approved by [your line manager OR the head of marketing AND / OR the managing partner].

6.6 The [head of marketing/IT/insert name] keeps a list of approved social media sites. This list can be found at [insert where list can be found]. You must not engage in social media activities on behalf of the firm on sites that are not shown in the approved list. If you wish to add a site to the approved list, you should contact the [head of marketing/IT/insert name].[[3]](#footnote-3)

6.7 You should not directly or indirectly represent the firm when using social media unless you are authorised [in writing] by [your line manager OR the head of marketing AND / OR the managing partner]. If you are not authorised to represent the firm, you should be clear that the opinions you express are yours alone and you should not:

6.7.1 use the firm's trade marks, brands or logos or other identifying material

6.7.2 quote the firm's name, email or other contact details[[4]](#footnote-4)

6.8 When engaging in social media activities in any way that could lead your activities to be associated with the firm you must:

6.8.1 act in a professional and responsible manner and exercise common sense, particularly bearing in mind any adverse impact your online activities might have on the firm's reputation or client relationships

6.8.2 ensure that your use of the firm’s logos and other branding material is consistent with [our marketing guidelines] and is approved by [the marketing department]

6.8.3 clearly identify who you are, including your name and job title [and also include contact details as appropriate]

6.8.4 ensure so far as possible you know who you are communicating with—beware of attempts to try to obtain passwords or user names from you in a way that may compromise security and ensure that you always log out of social media sites, particularly if you share a machine with other colleagues

6.8.5 ensure all arrangements with third parties in relation to your use of social media (eg online advertising, search engine optimisation or other arrangements) are properly documented, notified and approved by the [IT manager OR IT partner OR marketing manager AND / OR COLP].

6.8.6 ensure your communications are professional in tone and not overly informal

6.8.7 link back to firm communications and sites as appropriate, to highlight our products and services

6.8.8 ensure all communications are of high quality (in terms of content and form) including being grammatically correct, accurate, objectively justifiable, reasonable and appropriate for the intended audience

6.8.9 respect the confidentiality of our clients and the firm—the table below gives examples of circumstances where you may inadvertently breach confidentiality by using social media:

|  |  |  |
| --- | --- | --- |
| Activity | Risk to confidentiality | Possible method to mitigate or avoid risk |
| You are a defendant medical negligence lawyer and you post a comment on your personal Facebook account that you will be visiting a particular medical centre the next day | The likely inference is that you are defending the medical practice or one of its practitioners in a medical negligence claim | Do not post any comment on a personal or private social media site that could lead to the inference that you are visiting a specific client, unless that client has given you express consent |
| You are engaged in a general discussion about a particular area of law and you post a comment that is clearly based on your own experience | Depending on how much information you have given, it may be easy to infer that you act or have acted for a particular client on the issue under debate | Be very careful when engaging in technical or other debates—be aware that by displaying your expertise, you may inadvertently disclose that you have acted for a particular client or in a particular case. Do not do so without express client consent |
| You are a matrimonial lawyer and you show a client as a business contact on a social media site | This could imply that the person concerned is a client—and for a matrimonial issue | It is difficult to see how to mitigate or avoid this risk, especially if you first made contact with the client via social media. It is not practical to prohibit linking to clients on social media sites.  You should therefore consider warning the client about the inference that may be drawn from your continued connection |
| You complete an online biography or CV with project names or details which could identify a client or client matter | You could identify a client or client matter | Consider whether it is necessary to seek the client's consent |

6.9 If you become aware of any criticism of the firm or comments you have transmitted via social media, you should draw this to the attention of the [marketing department OR marketing manager OR COLP]. Do not respond without the express consent of the [marketing department OR marketing manager OR COLP].

6.10 This policy does not seek to regulate your use of social media in a purely private capacity provided this has no bearing on the firm or its activities.

6.11 Be aware that any comments you make on a personal social media account could be in the public domain and may be associated with your employment. You may wish to monitor the privacy settings on any personal social media accounts that you hold to restrict the people who can read your comments. You may also wish to review the content of your personal social media accounts on a regular basis and delete anything that could reflect negatively on you in a professional capacity or on the firm.

6.12 We may monitor your use of social media in accordance with this policy.

6.13 We will also monitor how the firm uses social media generally and what is said about us and about our competitors. [Insert name or role of person responsible for monitoring] is responsible for this monitoring. The table at [Appendix 1](#ukContentItemfe6745f2-6a8e-4c06-b9ca-b6) contains examples of our monitoring methods. We will usually monitor on a [weekly OR monthly OR quarterly] basis.

6.14 [insert name or role ] is responsible for dealing with any incident involving social media.[[5]](#footnote-5)

Telephone and fax use

7.1 Our telephone and fax system is intended and should be used for business purposes. Reasonable personal use of the telephone and fax facilities will be allowed provided that it does not interfere with the performance of your duties and the terms of this policy are strictly adhered to.

7.2 You should exercise the same care when using the telephone or fax as when using email or other forms of written communication.

7.3 We may monitor your use of the firm's email telephone and fax system in accordance with this policy.

Personal use

8.1 You may use the internet and other electronic communication systems (including social networking sites) for your own personal use, provided you do so in accordance with this policy and that your personal use:

8.1.1 is kept to a minimum (both in terms of time spent and frequency)

8.1.2 does not interfere with your job performance or impact on office working hours

8.1.3 does not have a negative impact on the firm in terms of cost, reputation or otherwise

8.1.4 is lawful

8.2 We may monitor personal use in accordance with this policy.

Misuse

9.1 You must not send offensive, demeaning, disruptive or defamatory messages or images via the internet, social media or any of our electronic communication systems. This includes, but is not limited to:

9.1.1 messages inconsistent with our Equality and diversity policy[and harassment policy]

9.1.2 any sexist or racist material

9.1.3 any material that could be offensive on the grounds of a person’s disability, age, sexual orientation, religion or belief

9.2 You must not place on the system or send any message or image that could be regarded as personal, potentially offensive or frivolous to any recipient or to any other person (even if not sent to them). If you receive an email, electronic message or a fax containing material that is offensive or inappropriate to the office environment you must delete it immediately. Under no circumstances should it be forwarded either internally or externally.

9.3 When using the firm’s electronic communications system, including the internet, or engaging in social media activities you must not:

9.3.1 copy, modify or encrypt data unless authorised to do so

9.3.2 use the firm's communications system (including via the internet) to conduct any business that is not the firm's business

9.3.3 send, post or otherwise disclose confidential information, trade secrets or other confidential data of the firm or our clients

9.3.4 [send chain letters, junk mail, unauthorised adverts or other trivial content including jokes, quizzes or video clips]

9.3.5 access or attempt to access another person's computer, computer account, email, files or other data without the express consent of the person concerned or the [Head of HR OR COLP]

9.3.6 access or attempt to access any password-protected or restricted parts of the firm's IT systems for which you are not an authorised user

9.3.7 download, copy or send any material that is protected by copyright or other intellectual property rights belonging to a third party without their permission

9.3.8 use the firm's IT or communications system for hacking, cracking, bugging, virus distribution, or access and/or tamper with systems or data without authorisation

9.3.9 send (inside or outside work) any message in the firm's name unless it is for a work-related purpose

9.3.10 use the firm's IT or communications system other than in accordance with this policy and any other of the firm's policies and procedures that may be relevant, eg equality and diversity policy

9.3.11 use the firm's logos and other branding material without the approval of the [marketing department OR marketing manager OR COLP].

9.3.12 not disclose financial information, client information, personal information or other information that could damage the firm or its reputation

9.3.13 not infringe any intellectual property or privacy rights of the firm or any third party—if you intend to mention a competitor directly then seek advice from [your line manager OR the marketing department OR the COLP] before doing so

9.3.14 provide references or recommendations for a third party, unless expressly authorised by the [marketing department OR marketing manager OR COLP]

9.3.15 make personal use of the firm’s telephone system for premium rate or international calls [unless expressly authorised by your supervisor]

Monitoring

10.1 All telephone and internet usage is logged automatically by the firm's computer system. Addresses of emails and internet sites visited are logged and the content of internet pages stored [state where this data is stored, eg on the firm's servers]. This is an automatic consequence of the way our computer system works. Except as set out in this policy, this data is not accessed or used in any way by any member of staff, other than for business continuity and IT housekeeping purposes.

10.2 We will monitor and keep records of your use of the email, telephone, fax and internet for a number of reasons:

10.2.1 ensuring compliance with the terms of this policy

10.2.2 investigating breaches and potential breaches of this and any other of the firm's policies

10.2.3 training and monitoring standards of service

10.2.4 accessing emails or voicemail messages in your absence for authorised business purposes

10.2.5 ensuring compliance with regulatory practices or procedures imposed or recommended by any regulatory body relevant to our business

10.2.6 ascertaining whether internal or external communications are relevant to the firm's business

10.2.7 preventing, investigating or detecting:

(a) unauthorised use of our IT and electronic communications systems

(b) misuse of our IT and electronic communications systems

(c) criminal activities

10.2.8 maintaining the effective operation of the firm's IT and electronic communication systems

10.2.9 locating and retrieving lost data[[6]](#footnote-6)

10.3 We do not as a matter of policy routinely monitor your use of the internet, social media or the content of email messages. However, there may be occasions when we need to access the content of a communication sent or received by you, or monitor the content of a telephone conversation for one of the reasons set out above.

10.4 Similarly, we may monitor which internet sites you visit and the time you spend visiting them. We may look at the content of the sites visited for one of the purposes set out above.

10.5 Unless clearly marked in the subject heading as being personal, we will assume that any emails sent using the firm's system are work-related and those emails (or any other form of communication using the internet) should not be considered private. You must not mark an email as personal when it is not, nor must you make excessive use of personal emails.

10.6 We reserve the right to read your emails while you are absent or out of the office to check for business emails. We may also access your voicemail to check for business calls while you are absent or out of the office. It may therefore be unavoidable that some personal messages will be read or heard.[[7]](#footnote-7)

Privacy and data protection

11.1 Information about others

11.1.1 It is likely that personal information relating to other individuals will come into your possession as a result of using our IT or electronic communications system, eg:

(a) general personal information, such as a client's address

(b) sensitive personal information, such as details of an illness

11.1.2 You should keep this information confidential and not disclose it unless you are authorised to do so. Ensure you process and handle personal data in accordance with our Data protection policy.

11.2 Information about you

11.2.1 We will hold and process your personal data in accordance with our Data protection policy.

11.2.2 We will retain a record of your use of the internet and electronic communications system for a maximum period of [[one year OR two years]] in accordance with our Data retention guidelines. These records will be kept secure and will be accessible only by the [IT manager OR IT partner OR Head of IT and other authorised personnel].[[8]](#footnote-8)

11.2.3 You are entitled to request a copy of these records. If you wish to do so, please contact [the HR department OR your line manager][We may charge a small fee for providing personal data about you as permitted by applicable law. This fee will be no more than £10.]. There are also restrictions on the information to which you are entitled under applicable law. For more guidance see our Data protection policy.[[9]](#footnote-9)

11.2.4 If you become aware that records of your use of the internet and electronic communications system are inaccurate, you may request that they are amended. If you wish to do so, please make a request in accordance with our Data protection policy. If we consider the amendment unnecessary, you can add a statement to qualify or counter the records in question.

11.2.5 In the event that these records are used as evidence in any disciplinary action against you, you will be given a chance to explain or challenge them.

11.2.6 If you have any queries in relation to your obligations or rights in relation to data protection, please contact the [data protection officer OR COLP]

Reporting breaches

12.1 All members of staff have an obligation to report actual or potential compliance failures. This allows us to:

12.1.1 investigate the failure and take remedial steps if necessary

12.1.2 maintain a register of compliance failures

12.1.3 notify the SRA of any compliance failures that are material either in their own right or as part of a pattern of failures

12.2 Please refer to our Compliance failure policy for our reporting procedure.

Consequences of breaching this policy

13.1 We consider this policy to be extremely important. Failure to comply puts both you and the firm at risk.

13.2 If you breach the policy it is very likely that you will be disciplined in accordance with our disciplinary procedure and may be dismissed.

13.3 In certain circumstances, breach of this policy may be considered gross misconduct resulting in immediate termination of employment without notice or payment in lieu of notice. As an alternative, we may withdraw your internet or email access.

Monitoring and review

14.1 The [IT manager OR IT partner OR COLP] is responsible for this policy.

14.2 We regularly monitor the effectiveness of this policy to ensure it is working in practice and we will review and update this policy as and when necessary.

14.3 We will review this policy regularly—at least annually. We will provide information and/or training on any changes we make.

Training

15.1 All staff will receive appropriate training on our Internet and electronic communications policy, including:

15.1.1 regular training for existing staff

15.1.2 training for new staff at induction

15.1.3 updates following any changes to the policy that affect staff

APPENDICES

1. Additional Note: Policy non-contractual

   Your policy should include any restrictions in employment contracts.

   Most firms will wish to ensure the policy does not have contractual force, to give them as much flexibility as possible in relation to amending the policy as they wish and departing from the procedures set out in the policy when it is appropriate to do so.

   See also [Law Society practice note: Social media, 20 December 2011](file:///\\Lnglondatp110\Users\OSWINJX\Word%20versions\www.lawsociety.org.uk\support-services\advice\practice-notes\social-media\) [↑](#footnote-ref-1)
2. Additional Note: Social media policy

   Your policy should include guidelines for engaging in social media, including how those guidelines will be communicated.

   See also: [Law Society practice note: Social media, 18 June 2015](file:///\\Lnglondatp110\Users\OSWINJX\Word%20versions\www.lawsociety.org.uk\support-services\advice\practice-notes\social-media\) [↑](#footnote-ref-2)
3. Additional Note: List of approved sites

   It will help you to manage risk to identify which social media sites the firm and its staff can utilise in a professional capacity. If you take this approach, you should review your list on a regular basis as social media is a fast paced environment; if not, you could inadvertently prevent your staff from using a new, highly effective site. [↑](#footnote-ref-3)
4. Additional Note: Staff not authorised to represent the firm

   Your policy should include guidelines on the use of disclaimers, eg that the views expressed are those of the employee and do not represent the firm.

   You may prefer to prohibit staff from engaging in social media activities that do not represent the views of the firm. Regardless of any disclaimer, you are likely to be associated with whatever opinion is being expressed.

   See also: [Law Society practice note: Social media, 18 June 2015](file:///\\Lnglondatp110\Users\OSWINJX\Word%20versions\www.lawsociety.org.uk\support-services\advice\practice-notes\social-media\) [↑](#footnote-ref-4)
5. Additional Note: Monitoring the firm’s social media activities, etc

   You should monitor social media sites to keep a careful eye on what is being said about your firm, your staff and your services. It also makes commercial sense to monitor your competitors activities in terms of their own marketing practices. Depending on the importance of social media, you may wish to consider:

   * appointing one person to coordinate your monitoring activities
   * stating the frequency of reviews—this will depend on how much you rely on social media
   * defining the main issues to monitor, eg:
     + - the social media activities that you have consciously engaged in as a business—what activities have you engaged in and are your activities on-brand and giving consistent a message?
       - any positive comments that have been posted about you—this could be by clients, third parties or your own staff
       - any negative comments
       - any potential confidentiality breaches
       - any other potential breach of your professional obligations
       - posts by or about your main competitors
       - posts by or about about key clients
       - whether the privacy settings have changed for any of the main sites you use or your staff may use (including in a personal capacity)
       - whether you should cease your activities in any particular area, eg sites that are not generating sufficient traffic and whether you should add any new sites to your approved list

   Realistically, this task will sit best with someone who has a genuine interest in social media, although that person may need some regulatory guidance from your COLP. There are external providers who can help you to monitor your own social media activities and what others say about you on social media, eg LexisNexis® Analytics. For a template monitoring form, see Lexis Nexis template: Social media activity monitoring form. [↑](#footnote-ref-5)
6. Additional Note: Reasons for monitoring

   It is important to know the difference between simple monitoring and intercepting an electronic communication because it is an offence to intentionally and without lawful authority intercept an electronic communication in the course of its transmission. This policy reflects exceptions that apply under the Regulation of Investigatory Powers Act 2000 (RIPA 2000), s 1(2) and Telecommunications (Lawful Business Practice)(Interception of Communications) Regulations 2000, SI 2000/2699, reg 3.

   For more guidance, see Lexis Nexis practice note: Monitoring staff; RIPA 2000, s 1(2) [↑](#footnote-ref-6)
7. Additional note: Monitoring staff

   Most employers will monitor their staff’s use of the internet, email and other electronic communications, such as social media. This is done to:

   * + - check that staff are not posting or receiving offensive material
       - ensure staff are not posting inappropriate messages
       - maintain basic IT security
       - monitor service
       - identify training needs
       - comply with regulatory requirements

   Failure to monitor these threats would leave the firm exposed to a variety of IT, employment and reputational risks.

   It is essential that you comply with the regulatory requirements on data protection and interception of electronic communications.

   For more guidance see practice note: Monitoring staff. Our template Internet and electronic communications policy incorporates the permitted methods of monitoring as described in ICO Employment Practices Code, supplementary guidance. For more guidance, see practice note: Monitoring amounting to an interception. [↑](#footnote-ref-7)
8. Additional note: Retaining data about staff

   See our template: Data retention guidelines, which is appended to our template: Data protection policy. Records relating to certain HR records are subject to statutory retention periods, eg your accident book, statutory Maternity Pay records and salary and pay records.

   There is no statutory retention period for records relating to your staff’s use of the internet and electronic communication system. It is up to you to decide how long to keep these records, but remember that personal data must not be kept longer than necessary. You should consider what would be a necessary retention period. [↑](#footnote-ref-8)
9. Additional note: Fees for granting subject access

   Charging a fee for granting subject access is not obligatory but you may charge the fee (up to a maximum of £10) for access. [↑](#footnote-ref-9)