IT Policy

1. Policy statement

1.1 Our electronic communications systems, internet usage and equipment are intended to promote effective communication and working practices within Muckle LLP ("the firm") and are critical to the success of our business. This policy outlines the standards we require users of these systems to observe, the circumstances in which we will monitor use of these systems and the action we will take in respect of breaches of these standards.

1.2 We reserve the right to monitor, intercept and review, without further notice, our people's activities using our IT resources and communications systems, including but not limited to social media postings and activities, to ensure that our rules are being complied with and for legitimate business purposes and you consent to such monitoring by your use of such resources and systems.

1.3 Compliance with this policy, as amended from time to time, is a condition of any employee's contract of employment and any breach of the terms of this policy will constitute a breach of the user's terms and conditions of employment and may result in disciplinary action being taken.

2. Who is covered by the policy?

2.1 This policy covers individuals working at all levels and grades, including partners, directors, employees, consultants, contractors, trainees, paralegals, home workers, part-time and fixed-term employees, casual and agency team members working for the LLP (collectively referred to as users in this policy).

2.2 Third parties who have access to our electronic communication systems and equipment (including but not limited to, Wi-Fi services) are also required to comply with this policy.

3. Scope and purpose of the policy

3.1 This policy deals mainly with the use (and misuse) of computer equipment, email, the internet, telephones, smartphones and voicemail, but it applies equally to the use of fax machines, copiers, scanners, and electronic key fobs and pass cards.

3.2 Users are expected to comply with this policy at all times to protect our electronic communications systems and equipment from unauthorised access and harm.

4. Roles and responsibilities

4.1 The Managing Partner has overall responsibility for the effective operation of this policy, but has delegated day-to-day responsibility for its operation to the Director of IT. Responsibility for monitoring and reviewing the operation of this policy and making any recommendations for change to minimise risks to our operations also lies with the Director of IT.

4.2 The IT team will deal with requests for permission or assistance under any provisions of this policy, subject to their primary tasks of maintaining our core systems, and may specify certain standards of equipment or procedures to ensure security and compatibility.

4.3 All managers have a specific responsibility to operate within the boundaries of this policy, ensure that all users understand the standards of behaviour expected of them and to take action when behaviour falls below its requirements.

4.4 All users are responsible for their own obligations under this policy and should ensure that they take the time to read and understand it. Any misuse of our electronic communications

systems or equipment should be reported to the Director of IT. Questions regarding the content or application of this policy should be directed to the Director of IT.

5. **Email**

5.1 All users have the technological capability to send and receive external emails.

5.2 Email is a vital business tool, but should be used with care and discipline. Users should always consider if email is the appropriate means for a particular communication and correspondence sent by email should be written as professionally as a letter or fax. The firm's housestyle and standards apply to email as they do to hard copy correspondence and the firm's footer disclaimer must not be amended or removed.

5.3 A contract formed by email is capable of forming a binding agreement in the same way as oral or written communications. Representations made by email may also be binding on the firm. Only specifically authorised users are entitled to conclude contracts or make representations by email.

5.4 Although the courts now allow litigation documents to be served by email in certain circumstances, the firm's general policy is that email should not be used for this. Users must not serve or accept service of litigation documents by email without first obtaining the specific consent of their supervising partner.

5.5 Email messages may be disclosed in legal proceedings in the same way as paper documents. Deletion from a user's mailbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable, either from the main email server, the email archiving system or the firm's cloud-based email filtering service.

5.6 The sender or recipient of an email is responsible for saving it to the relevant client folder within the Document Management System (DMS) and the hard copy filing of that email where necessary. It is essential that emails are electronically archived. Guidance for users is available on the firm's intranet regarding its use. All users shall comply with such guidance when using the DMS. Non-compliance with these guidance notes may result in the instigation of disciplinary procedures.

5.7 All users should ensure that they routinely file and delete emails as appropriate. The "deleted items" folder is automatically cleared every time MS Outlook is closed.

5.8 Trainees should only send emails that have not been approved by a lawyer (with a current practicing certificate) where they have had permission to do so from the lawyer supervising the relevant file. Except where an external email is purely administrative (e.g. booking a course or confirming an appointment) secretaries must have external emails approved by the lawyer for whom they are working before sending.

5.9 Emails must not contain insulting, aggressive or discriminatory language or defamatory comments. In particular, the email system must not be used to transmit, store or display material that is:

5.9.1 racially or religiously offensive, biased or discriminatory in any way;
5.9.2 obscene, indecent, sexually suggestive (including, pornographic material of any kind);
5.9.3 abusive or threatening;
5.9.4 false, inaccurate, or a violation or infringement of any other person's right to privacy;
5.9.5 relates to any criminal or otherwise illegal activity;
5.9.6 for the purpose of conducting any unauthorised business, in particular personal business transactions; or

5.9.7 for the purpose of knowingly transmitting a virus, worm or other malware which is likely to cause damage to the firm's or a third party's IT system.

5.10 In general, users should not:

5.10.1 send or forward private emails at work which they would not want a third party to read;
5.10.2 send or forward chain mail, junk mail, cartoons, jokes, gossip or emails that contain derogatory comments about an individual or comments that may cause offence to a third party; or
5.10.3 send messages from another worker's computer or under an assumed name unless specifically authorised.

5.11 Email must not be used in a way that causes a waste of time, resources or contribution to system congestion. Messages should be distributed only to those individuals or groups to whom they will be meaningful and useful and must not be sent to the Muckle team email distribution group or other large groups when they are irrelevant to many of the people in that group.

5.12 Users must not (unless specifically authorised by the Director of IT) store or transmit video and animation files, pictures files, sound files or program files.

5.13 Users are not permitted to use the firm's systems to set up or use personal webmail accounts such as Hotmail.

5.14 The confidentiality of emails cannot be guaranteed. Users must therefore consider carefully whether it is appropriate to send confidential material by email and in particular should check with clients that they are willing to receive material in this way. Users who are in any doubt should consult their group head or line manager.

5.15 Emails incorporating confidential information must not be disclosed to unauthorised persons and under no circumstances should sensitive personal data (including but not limited to, medical information) be sent by email to third parties.

5.16 If a user wants to ensure confidentiality of correspondence relating to his/her health, or any other sensitive issues e.g. sickness absence, BUPA or PHI information, then this correspondence should be delivered by hand to the relevant person or dealt with by telephone rather than by email.

5.17 Users should use CipherMail for sending encrypted emails unless the intended recipient has a recognised preferred solution.

6. Internet

6.1 Internet access is available to all users for business purposes at any time.

6.2 Users must not download or print material (including images, documents and music) from the internet, unless they do so in accordance with a copyright notice on the material or they have obtained the copyright owner's permission. Even if a document is not marked with a copyright notice the document may still be copyright protected. Infringement of copyright is a serious matter which may result in civil or criminal penalties. Therefore if users are in any doubt, they must not download or print the material.

6.3 When a website is visited, devices such as cookies or tags may be employed to enable the site owner to identify and monitor visitors. If the website is of a kind described in paragraph 15.1, such a marker could be a source of embarrassment to the visitor and us, especially if

inappropriate material has been accessed, downloaded, stored or forwarded from the website.

6.4 Users should not access (even during permitted personal time) any web page or any files from the internet which could, in any way, be regarded as illegal, offensive, in bad taste or immoral. While content may be legal in the UK, it may be in sufficient bad taste to fall within this prohibition. As a general rule, if any person (whether intended to view the page or not) might be offended by the contents of a page, or if the fact that our software has accessed the page or file might be a source of embarrassment if made public, then viewing it will be a breach of this policy.

6.5 All internet usage (for business purposes or otherwise) is filtered by third party software and may be further monitored in accordance with paragraph 14.

6.6 Users should be aware that use of our systems is controlled and monitored by third party software that allows the firm's IT team to restrict access to certain categories of websites (as well as specific sites).

6.7 Users should not under any circumstances use our systems to participate in any internet chat room, post messages on any internet message board or set up or log text or information on a blog or wiki, even in their own time, unless for authorised business use.

6.8 Clients and external visitors may have access to the internet via a wireless network for their own purposes and using their own Wi-Fi-enabled device. This network is unrestricted, unfiltered and unmonitored by the firm. Users are not permitted to use our wireless network in any way that is unlawful or fraudulent, or to knowingly transmit any data, send or download any material that contains viruses, malware or any other harmful programs designed to adversely affect the operation of any computer software or hardware. Public Muckle LLP Wi-Fi users must accept the usage policy presented to them in their web browser before they are granted access to the internet.

6.9 The firm’s hardware is available to loan to clients whilst on the firm's premises for the purpose of accessing Wi-Fi services (subject to availability and the discretion of the Director of IT).

6.10 In no event will we be liable for any loss or damage whatsoever arising from any viruses or other technologically harmful material that may be sent, downloaded or transmitted by any external users, which may adversely affect the hardware or software of external users.

7. Security and risk

7.1 Users are responsible for the security of the equipment allocated to or used by them, and must not allow it to be used by anyone other than in accordance with this policy.

7.2 No-one may use the firm's network until they have been authorised and allocated a user name and password. Individuals without authorisation should only be allowed to use terminals under supervision.

7.3 The set up, administration and closing of Windows user accounts is the responsibility of the IT team. The procedures is fully documented and kept up to date.

7.4 The firm’s IT business continuity plan is tested every 3 months.

7.5 The firm uses HEAT for anti-virus and security patch management purposes. The latest anti-virus agent is deployed to all endpoint every 8 hours. Security patches are deployed to all Windows servers every 14 days.

7.6 All network hardware (including next generation firewalls, storage area networks and servers) and software is installed and configured in line with industry standards. Intrusion detection and associated alerting is enabled on the firewalls. Where necessary professional services of trusted 3rd party support companies are employed for the setup and configuration purposes. All such Muckle hardware is securely stored at Time Central, NE1 4BF, Aspire Technology Solutions Ltd, NE10 0UX and First Storage, NE10 0AZ.

7.7 Any security or cyber incident should be reported to the Director of IT. The appropriate action will then be taken.

7.8 Client matter inception (CMI) is the firm's process for opening new matters. Part of this process includes the automatic creation of a matter workspace within the DMS. Security on workspaces is assigned as public unless explicitly indicated during CMI. E.g. banking matters are generally marked as private.

7.9 Users are responsible for the security of their terminals. If leaving a terminal unattended, users should ensure that they secure their terminal by either logging off or pressing the CTRL+ALT+DELETE keys together and selecting the 'lock computer' option to prevent unauthorised users accessing the system in their absence. All users must shut down their workstation and turn off their monitor when leaving the office for the day.

7.10 Desktop PCs and cabling for telephones or computer equipment should not be moved or tampered with without first consulting a member of the IT team. Only authorised members of the IT team may connect hardware to the network.

7.11 It is the responsibility of each user to keep their password confidential. Passwords must not be made available to anyone else. That said, you may be asked for your password on occasion by a member of the IT team to facilitate the delivery of support to you. If you share your password with a member of the IT team you should change it as soon as the work is completed by IT. The following guidelines in relation to passwords must be strictly adhered to:

7.11.1 passwords must be a minimum of 9 characters;

7.11.2 they must not contain an account name or part of the user's full name that exceeds two consecutive characters (i.e. John Smith could not have the password smi123456% as the first three characters are the same as his surname);

7.11.3 they must contain characters from three of the following four categories for added complexity:

7.11.3.1 English uppercase characters (A through Z);

7.11.3.2 English lowercase characters (a through z);

7.11.3.3 numbers (0 through 9);

7.11.3.4 non-alphabetic characters (for example: !, $, #, %).

7.11.4 a useful method for choosing a complex password is for it to be a phrase with symbols or numbers replacing certain letters e.g. 1lov3worK!;

7.11.5 passwords should not incorporate the name of a spouse, child or pet and should never be written down (particularly when taking equipment off site, e.g. a laptop for an external presentation or for home working);

7.11.6 users must change their password if it is suspected that it has been compromised. This can be done at anytime once logged in by pressing the CTRL+ALT+DELETE keys together and then choosing the "change password" option.

7.12 Users who have been issued with a laptop, PDA or smartphone must ensure that it is kept secure at all times, especially when travelling. Passwords must be used to secure access to data kept on such equipment to ensure that confidential data is protected in the event of loss or theft. Users should also be aware that when using equipment away from the workplace, documents may be read by third parties, for example, passengers on public transport and must take all reasonable steps to avoid such accidental disclosure.

7.13 Users using laptops or Wi-Fi enabled equipment must be particularly vigilant about its use outside the office and take any precautions deemed necessary by the IT team to avoid importing viruses or compromising the security of the system. The system contains information which is confidential to our business and/or which is subject to data protection legislation. Such information must be treated with extreme care and in accordance with our Data Protection Policy, which can be found on the firm intranet.

7.14 Care must be taken (whether on or off-site) to reduce the risk of liquids or food being spilled over any equipment. Any damage to computer equipment must be notified to the IT team, who will deal with any maintenance issues.

7.15 All equipment and data belonging to the firm must be treated with care, properly used for authorised purposes only and surrendered to the Director of IT upon the user leaving the employment of the firm.

7.16 Users should not delete, destroy or modify existing systems, programs, information or data which could have the effect of harming the firm or exposing it to risk.

7.17 Users should not download or install software including, but not limited to, software programs, games, instant messaging programs, screensavers, photos, video clips and music files except when authorised to do so for work purposes.

7.18 No device or equipment should be attached to our systems without the prior approval of the IT team. This includes any USB flash drive, MP3 or similar portable device, PDA, smartphone or telephone. It also includes use of a USB port, Bluetooth connection port or any other port.

7.19 If a user requires a USB flash drive for business purposes, the IT team will provide a secure encrypted device for this purpose.

7.20 Users should not attempt to gain access to restricted areas of the network, or to any password-protected information, unless specifically authorised. Only authorised personnel are permitted to enter the IT server room.

7.21 Use of the SMS facility on firm issued mobile phones or smartphones for the purpose of client contact is discouraged and should only be undertaken with care.

7.22 Only smartphones or mobile devices issued by the firm may be used to access the firm's systems (including email). Under no circumstances are users permitted to use their personal mobile devices to access firm systems.

7.23 Third party support organisations and contractors accessing data (whether personal or otherwise) held by the firm must have signed an appropriate non-disclosure agreement before access is granted.

7.24 Landline voicemail messages may be listened to in any user's absence. In addition, voicemail messages will be converted to .wav sound files and automatically emailed to that user's email account.

8. Remote access

8.1 All users can use Microsoft Outlook Web Access for email, calendar and task management. Guidance notes can be found on the intranet.

8.2 Nominated users are entitled to access the firm's systems (including the DMS) remotely using VMware View with RSA authentication. Guidance on accessing the firm's systems remotely can be found on the firm's intranet. In using the remote access facility, users shall:

8.2.1 immediately report any incident which might compromise firm security;
8.2.2 avoid use of facilities in public places where possible;
8.2.3 not leave laptops unattended and under no circumstances, leave in a vehicle overnight; and
8.2.4 not leave user IDs and passwords or other security codes in hard copy form with laptops.

8.3 Where home working equipment is lost or damaged the Director of IT should be contacted immediately.

8.4 Remote access to the firm's systems will be monitored by the Managing Partner and/or the Director of IT from time to time in accordance with paragraph 14 in order to ensure the security of the firm's systems and to help prevent and/or detect unauthorised access to, or use of, the firm's systems.

9. Social media

9.1 Access to social networking and blogging sites from the firm's desktop PCs is restricted however sites which facilitate business networking (such as Linkedin) are accessible and usage may be monitored.

9.2 Users should refer to the firm's social media policy for guidance on usage.

10. Aderant

10.1 Use of Aderant must be in compliance with the training and guidance given during training.

11. Training

11.1 All users are given the necessary software, hardware and procedural training to allow them to fulfil their role in the firm.

11.2 On joining the firm all users at given information security training. This includes how to spot and dealing with phishing emails. Such training is ongoing and reinforced by running periodic phishing simulation exercises.

12. Information retention and disposal

12.1 Debt collection, County Court litigation, crime, contentious construction data is retained for 7 years.

12.2 Commercial and residential property, commercial transactions, probate, secured lending (unless mortgage has been discharged earlier), partnership agreements, company formation, patents/intellectual property matters, wills, non contentious construction is retained for 15 years.

12.3 It must be considered on a matter by matter basis if circumstances warrant a file being kept longer than the periods listed in 12.1 and 12.2. If in doubt err on the side of caution. If you are unclear as to the period the paper / electronic file should be retained for speak to Judith Birkett or Kirsty Orr.

13. Personal use of systems

13.1 Access is granted to the internet, telephones and other electronic systems for legitimate business purposes only. Incidental personal use is permissible provided it is in full compliance with the firm's rules, policies and procedures and in particular, this clause 13.

13.2 The internet, email and telephone systems may be used to send personal email, browse the internet and make personal telephone calls subject to certain conditions set out below. Personal use is a privilege and not a right. It must be neither abused nor overused and we reserve the right to withdraw our permission at any time.

13.3 The following conditions must be met for personal usage to continue:

13.3.1 use must be minimal and take place substantially out of normal working hours (that is, during the user's lunch break, before 9am or after 5pm);
13.3.2 personal usage of emails must not exceed 10 personal emails or 5% of a user's hours per day (whichever is the lesser);
13.3.3 personal emails must be labelled "personal" in the subject header;
13.3.4 use must not interfere with business or office commitments;
13.3.5 use must not commit us to any marginal costs; and
13.3.6 use must comply with this and other associated policies.

13.4 A user's personal webmail may (at the Director of IT's sole discretion) be checked on a laptop held by the IT team.

13.5 Personal use of firm issued mobile phones and smartphones (and other portable devices) is permitted so far as such use complies with the terms of this policy. Bills are reviewed by the Director of IT and any personal use that the Director of IT deems excessive may result in the user being billed, disciplinary action being taken and/or a requirement to surrender the device.

13.6 The backup of personal data on Muckle smartphones is not the responsibility of the firm. The firm can, without notice, wipe any Muckle smartphone. Such a wipe will indiscriminately purge all data (corporate & personal) from the device. Purged data cannot be recovered.

13.7 The firm is not liable for any personal data lost following the wipe of a Muckle smartphone.

13.8 Where breaches of this policy are found, action may be taken under the firm's disciplinary procedures. The firm reserves the right to restrict or prevent access to certain telephone numbers or internet sites if it is considered that personal use is excessive.

14. Monitoring of use of systems

14.1 For business purposes, and to prevent unauthorised use of the firm's IT systems, the firm expressly reserves the right to monitor the number of personal emails sent by users, the time spent by users using the internet and to carry out spot checks on the internet sites visited by users at its absolute discretion. However, personal use of the internet will not be monitored except in circumstances where users are suspected of using the facilities for purposes which no reasonable employer would ignore (for example, excessive use or where usage is affecting service delivery).

14.2 The firm respects the privacy of users of its email system. Emails marked as 'personal' will not be opened and the content will not be read by anyone within the firm except in limited circumstances where there are bona fide reasons for doing so, for example if the user is suspected of using email to harass other users or to the detriment of the firm.

14.3 Emails which are not marked as 'personal' may be routinely monitored, accessed, opened and read by team managers, the Director of IT and the Managing Partner in order to prevent or detect criminal activity, prevent unauthorised use of the IT systems, to monitor and record business transactions, to ensure the effective smooth running of the IT systems, to ensure regulatory compliance, to maintain quality controls and/or to assess training needs.

14.4 The firm monitors all emails passing through its system for viruses. Users should exercise caution when opening emails from unknown external sources or where, for any reason, an

email appears suspicious. The IT team should be informed immediately if a suspected virus is received. The firm reserves the right to block access to attachments to emails for the purpose of effective use of the system and for compliance with this policy. It also reserves the right not to transmit any email message.

14.5 PAs are able to access the email inbox and sent items of their respective lawyers and lawyers within their respective group. They are authorised to open and read emails not marked as 'personal' in order to ensure that relevant correspondence can be dealt with if their lawyer(s) is / are not in the office or is / are unavailable. Head PAs are authorised to access any lawyer's email folders to ensure business continuity, for example in the event of sickness absence.

14.6 All emails received from external services may be monitored, accessed, opened and read unless it is entirely clear from the subject header that they are personal emails. Users should inform those who may use email to contact them at work for personal purposes that their emails may be monitored.

14.7 All emails sent and received, whether internal or external, are recorded in the firm's email archiving system. This data is kept indefinitely regardless of whether the original email has been deleted from the user's Outlook mailbox.

14.8 The firm reserves the right to retrieve the contents of messages or check searches which have been made on the internet for the following purposes (this list is not exhaustive):

14.8.1 to monitor whether use of the email system on the internet is legitimate and in accordance with this policy;
14.8.2 to find lost messages or to retrieve messages due to computer failure;
14.8.3 to assist in the investigation of wrongful acts; or
14.8.4 comply with any legal obligation.

15. **Inappropriate use of equipment and systems**

15.1 Misuse or excessive use or abuse of our telephone or email system, or inappropriate use of the internet in breach of this policy will be dealt with under the firm's disciplinary procedure. Misuse of the internet can, in certain circumstances, constitute a criminal offence. In particular, misuse of the email system or inappropriate use of the internet by creating, viewing, accessing, transmitting or downloading any of the following material will amount to gross misconduct (this list is not exhaustive):

15.1.1 pornographic material (that is, writing, pictures, films and video clips of a sexually explicit or arousing nature);
15.1.2 offensive, obscene, or criminal material or material which is liable to cause embarrassment to us or to our clients;
15.1.3 gambling;
15.1.4 a false and defamatory statement about any person or organisation;
15.1.5 material which is discriminatory, offensive, derogatory or may cause embarrassment to others;
15.1.6 confidential information about us or any of our people or clients (which you do not have authority to access);
15.1.7 any other statement which is likely to create any liability (whether criminal or civil, and whether for you or us);
15.1.8 material in breach of copyright; or
15.1.9 knowingly transmitting a virus, worm or other malware which is likely to cause damage to the firm's or a third party's IT system.

Any such action will be treated very seriously and is likely to result in summary dismissal.

15.2 Users should be aware of the potentially harmful effects of computer viruses on the firm's systems, or networks belonging to third parties. Viruses are programs written specifically to corrupt other programs or data files and can cause disruption and damage to the system before they are detected. Many are introduced by way of email and attachments. Viruses are also introduced through CDs and USB memory sticks and other portable media from outside the firm. Any such media will be checked automatically by the anti-virus software on all PCs prior to use. Those checking systems must not be disabled by users. The IT team should be informed of any unexpected anti-virus program behaviour. All inbound email is also scanned by a third party cloud-based service called Mimecast. This service helps protect the firm against viruses as well as spam and phishing emails.

15.3 On discovering a virus, the user must contact the IT team immediately to prevent any permanent damage to or loss of data.

15.4 The Computer Misuse Act 1990 (CMA) was introduced to combat computer hacking, electronic eavesdropping and virus infection. Breaches of the CMA are punishable by fine, imprisonment or both. Users must abide by the terms of the CMA, and in particular must not:

15.4.1 use any computer equipment without permission;
15.4.2 try to access information unless specifically authorised; and
15.4.3 modify information on a computer system unless specifically authorised.

15.5 Software is protected by copyright. It is illegal to copy software without the copyright owner's permission. For that reason only software authorised by the firm which is legally licensed may be used on the firm's IT systems. Audits of software and hardware are carried out periodically. Any unlicensed or unauthorised software will be removed. This prohibition includes screensavers and games. A list of all software used by the firm can be found in Appendix 1. All software is maintained on a version that is compatible with all other Muckle systems. Deployed software is managed via Group Policy and is regularly audited via Spiceworks.

15.6 Users must not access the firm's systems or use the firm's equipment (on firm premises or otherwise) when intoxicated by alcohol or other drugs.

15.7 Any behaviour which is in breach of this policy (as amended from time to time), brings the firm into disrepute or negatively impacts upon employees, members, business partners or clients may be treated as a disciplinary offence and could result in disciplinary action (including dismissal) being taken.

16. Monitoring and review of this policy

16.1 The Director of IT in conjunction with the Managing Partner shall be responsible for reviewing this policy to ensure that it meets legal requirements and reflects best practice.

16.2 The Director of IT has responsibility for ensuring that any person who may be involved with administration or investigations carried out under this policy receives regular and appropriate training to assist them with these duties.

17. Breach management

17.1 Any loss of equipment or data must be reported to the Director of IT immediately so that steps may be taken to mitigate the loss. If any such loss takes place outside of normal hours, users should contact the Director of IT on 07833 240 436 or the Managing Partner on 07850 508 301.

17.2 Where the data breach involves theft of equipment, the IT team shall report such theft to the police (and the insurers and/or clients involved where relevant and appropriate).

17.3 All breaches of data security (whether caused by loss or damage of equipment, virus or other unauthorised access to systems and or data) will be reported to the Managing Partner by the Director of IT, who will decide what action (including investigation and disciplinary action where appropriate) will be taken.

18. **Security change management**

18.1 User access to DMS workspaces is determined by role in the firm.

18.2 Changes to such permissions must be sent to IT via email and authorised by a users' line manager.

Appendix 1
A list of all applications used by the firm

1. MS Outlook 15.0.4569.1506
2. MS Word 15.0.4569.1506
3. MS Excel 15.0.4569.1506
4. MS PowerPoint 15.0.4569.1506
5. MS Publisher 15.0.4569.1506
6. MS Visual Studio 2010 for office 10.0.50908
7. MS Visio Viewer 14.0.7015.1000
8. MS Internet Explorer 11
9. InforCRM 8.2.0.1374
10. Laserform 9.6
11. Hotdocs 10.03.2550
12. BigHand 4.22.1
13. iManage Worksite 9.1
14. TightVNC 2.0.3
15. EAS Client 6.4.0
16. HEAT anti-virus 8.5.0.10
17. Adobe Reader DC 2015.023.20056
18. Open Office 3.3.9567
19. eCopy PDF Pro Office 6.3
20. Dragon Naturally Speaking 13.00.000
21. JCT Contracts 1.00.0000
22. Liberate 1.00.000
23. GIMP 2.8.20
24. Aderant Expert 8.5 SP1
25. compareDocs 4.2.300.9
26. Adobe Creative Suite 2017.1.1

All applications are monitored and kept up to date for support and security purposes.