COLORMINIUM
LONDON

IT and Communications Systems Policy

1. About this policy

1.1. Our IT and communications systems are intended to promote effective communication and working practices within our organisation. This policy outlines the standards you must observe when using these systems, the circumstances in which we will monitor your use, and the action we will take in respect of breaches of these standards.

1.2. This policy covers all employees, officers, consultants, contractors, casual workers, agency workers and anyone who has access to our IT and communication systems.

1.3. Misuse of IT and communications systems can damage the business and our reputation. Breach of this policy may be dealt with under our Disciplinary Procedure and, in serious cases, may be treated as gross misconduct leading to summary dismissal.

1.4. This policy does not form part of any employee's contract of employment and we may amend it at any time.

2. Equipment security and passwords

2.1. Everyone who works for, or on behalf of, the Company has some responsibility for ensuring data is collected, stored and handled appropriately, in line with this Policy and the Company's Data Security and Data Retention policies.

2.2. You should only access personal data covered by this Policy if you need it for the work you do for, or on behalf of the Company and only if you are authorised to do so. You should only use the data for the specified lawful purpose for which it was obtained.

Saxon House, 23 Springfield Lyons Approach, Chelmsford, CM2 5LB
+44(0)1245 658 268 | info@colorminium.com | Company No: 07199913 | VAT No: GB 199391547

2.3. You should regularly review and update personal data which you have to deal with for work. This includes telling us if your own contact details change.

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

2.5. You are responsible for the security of any computer terminal used by you. You should lock your terminal or log off when

leaving it unattended or on leaving the office, to prevent unauthorised users accessing the system in your absence.

2.6. You should use strong passwords on all IT equipment, particularly items that you take out of the office. You must keep your passwords confidential at all times. On the termination of employment (for any reason) you must provide details of your passwords to the IT Manager and return any equipment, key fobs or cards.

2.7. If you have been issued with a laptop, PDA or BlackBerry, you 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. You 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.

3. Systems and data security

3.1. You should not delete, destroy or modify existing systems, programs, information or data (except as authorised in the proper performance of your duties).

3.2. You must not download or install software from external sources without authorisation from the IT Manager.

Saxon House, 23 Springfield Lyons Approach, Chelmsford, CM2 5LB
+44(0)1245 658 268 | info@colorminium.com | Company No: 07199913 | VAT No: GB 199391547

3.3. We monitor all e-mails passing through our system for viruses. You should exercise particular caution when opening unsolicited e-mails from unknown sources or an e-mail which appears suspicious (for example, if it contains a file whose name ends in .exe). Inform the IT Manager immediately if you suspect your computer may have a virus. We reserve the right to delete or block access to e-mails or attachments in the interests of security. We also reserve the right not to transmit any e-mail message.

3.4. You should not attempt to gain access to restricted areas of the network, or to any password-protected information, except as authorised in the proper performance of your duties.

3.5. If you use laptops or wi-fi enabled equipment, you must be particularly vigilant about its use outside the office and take such precautions as we may require from time to time against importing viruses or compromising system security. 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.

4. E-mail

4.1. You must not send abusive, obscene, discriminatory, racist, harassing, derogatory, defamatory, or otherwise inappropriate emails. Anyone who feels that they have been harassed or bullied, or are offended by material received from a colleague via e-mail should inform their manager.

4.2. E-mail messages may be disclosed in legal proceedings in the same way as paper documents. Deletion from a user's inbox or archives does not mean that an e-mail cannot be recovered for the purposes of disclosure. All e-mail messages should be treated as potentially retrievable, either from the main server or using specialist software.

4.3. In general, you should not:

Saxon House, 23 Springfield Lyons Approach, Chelmsford, CM2 5LB
+44(0)1245 658 268 | info@colorminium.com | Company No: 07199913 | VAT No: GB 199391547

4.3.1. send or forward private e-mails at work which you would not want a third party to read;

4.3.2. send or forward chain mail, junk mail, cartoons, jokes or gossip;

4.3.3. send messages from another person's e-mail address (unless authorised) or under an assumed name;

4.3.4. or send confidential messages via e-mail or the internet, or by other means of external communication which are known not to be secure.

4.3.5. Do not use your own personal e-mail account to send or receive e-mail for the purposes of our business. Only use the e-mail account we have provided for you.

5. Using the internet

5.1. When a website is visited, devices such as cookies, tags or web beacons may be employed to enable the site owner to identify

and monitor visitors. If the website is of a kind described in paragraph 8.3, 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. Such actions may also, in certain circumstances, amount to a criminal offence if, for example, the material is pornographic in nature.

6. Personal use of our systems

6.1. We permit the incidental use of internet, e-mail and telephone systems to send personal e-mail, 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 not be overused or abused. We may withdraw permission for it at any time or restrict access at our discretion.

6.2. You should be aware that personal use of our systems may be monitored (see paragraph 7) and, where breaches of this policy are found, action may be taken under the disciplinary procedure

(see paragraph 8). We reserve the right to restrict or prevent access to certain telephone numbers or internet sites if we consider personal use to be excessive.

6.3. You should not make unnecessary copies of personal data and should keep and dispose of any copies securely.

6.4. High risk personal data should be encrypted before being transferred electronically to authorised external contacts.

7. Monitoring

7.1. For business reasons, and in order to carry out legal obligations in our role as an employer, use of our systems including the telephone and computer systems, and any personal use of them, may be continually monitored by automated software or otherwise. Monitoring is only carried out to the extent permitted or as required by law and as necessary and justifiable for business purposes.

7.2. We reserve the right to retrieve the contents of e-mail messages or check internet usage (including pages visited and searches

made) as reasonably necessary in the interests of the business, including for the following purposes (this list is not exhaustive):

7.2.1. to monitor whether the use of the e-mail system or the internet is legitimate and in accordance with this policy;

Saxon House, 23 Springfield Lyons Approach, Chelmsford, CM2 5LB
+44(0)1245 658 268 | info@colorminium.com | Company No: 07199913 | VAT No: GB 199391547

7.2.2. to find lost messages or to retrieve messages lost due to computer failure;

7.2.3. to assist in the investigation of alleged wrongdoing; or

7.2.4. to comply with any legal obligation.

8. Prohibited use of our systems

8.1. 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 our rules, policies and procedures (including this policy, the Equal Opportunities Policy, Anti-harassment Policy, Data Protection Policy and Disciplinary Procedure). See paragraph 6, Personal use of systems.

8.2. Misuse or excessive personal use of our telephone or e-mail system or inappropriate internet use will be dealt with under our Disciplinary Procedure. Misuse of the internet can in some circumstances be a criminal offence. In particular, misuse of the

e-mail system or inappropriate use of the internet by participating in online gambling or chain letters or by creating, viewing, accessing, transmitting or downloading any of the following material will usually amount to gross misconduct (this list is not exhaustive):

8.2.1. pornographic material;

8.2.2. offensive, obscene, or criminal material or material which is liable to cause embarrassment to us or to our clients;

8.2.3. a false and defamatory statement about any person or organisation.

Saxon House, 23 Springfield Lyons Approach, Chelmsford, CM2 5LB
+44(0)1245 658 268 | info@colorminium.com | Company No: 07199913 | VAT No: GB 199391547

8.2.4. material which is discriminatory, offensive, derogatory or may cause embarrassment to others;

8.2.5. confidential information about us or any of our staff or clients (except as authorised in the proper performance of your duties);

8.2.6. any other statement which is likely to create any criminal or civil liability (for you or us); or

8.2.7. material in breach of copyright.

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

8.4. Where evidence of misuse is found we may undertake a more detailed investigation in accordance with our Disciplinary Procedure, involving the examination and disclosure of monitoring records to those nominated to undertake the investigation and any witnesses or managers involved in the Disciplinary Procedure. If necessary such information may be handed to the police in connection with a criminal investigation.

9. Personal data

9.1. Personal data should never be transferred outside the European Economic Area except in compliance with the law and authorisation of the Human Resources Department.

9.2. You should lock all drawers, cupboards and filing cabinets that contain personal data. Do not leave paper with personal data lying about.

Saxon House, 23 Springfield Lyons Approach, Chelmsford, CM2 5LB
+44(0)1245 658 268 | info@colorminium.com | Company No: 07199913 | VAT No: GB 199391547

9.3. You should ask for help from our Human Resources Department if you are unsure about data protection or if you notice any areas of data protection or security we can improve upon

9.4. Any deliberate or negligent breach of this Policy by you may result in disciplinary action being taken against you in accordance with our Disciplinary Policy.

9.5. It is a criminal offence to conceal or destroy personal data which is part of a subject access request (see below). This conduct would also amount to gross misconduct under our disciplinary procedure, which could result in your dismissal.

Saxon House, 23 Springfield Lyons Approach, Chelmsford, CM2 5LB
+44(0)1245 658 268 | info@colorminium.com | Company No: 07199913 | VAT No: GB 199391547