77 Elmers End Road, London, SE20 7UU . Tel: 020 8778 6111 . Fax 0208 778 5060 . Email: general@ddclimited.com

Davies Design and Construction Ltd - 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. This policy outlines the standards you must observe when using these systems, when we will monitor their use, and the action we will take if you breach these standards.

1.2 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.

2. Equipment security and passwords

2.1 Employees at DDC Ltd must access a variety of IT resources, including computers and other hardware devices, data storage systems, and other accounts. Passwords are a key part of IT's strategy to make sure that only authorised people can access those resources and data.

2.2 The purpose of this policy is to ensure that all DDC resources and data receive adequate password protection. This policy covers all employees who are responsible for one or more account or have access to any resource that requires a password.

2.3 You are responsible for the security of the equipment allocated to or used by you, and you must not allow it to be used by anyone other than in accordance with this policy. You should use password on all IT equipment, particularly items that you take out of the office. You should keep your passwords confidential and change them regularly.

2.4 You must only log on to our systems using your own username and password. You must not use another person's username and password or allow anyone else to log on using your username and password.

2.5 If you are away from your desk you should log out or lock your computer. You must log out and shut down your computer at the end of each working day.

2.6 All passwords should be reasonably complex and difficult for unauthorised people to guess. Employees should choose passwords that are at least eight characters long and contain a

77 Elmers End Road, London, SE20 7UU . Tel: 020 8778 6111 . Fax 0208 778 5060 . Email: general@ddclimited.com

combination of upper and lower-case letters, number and punctuation marks and other special characters. These requirements will be enforced with software when possible.

2.7 In addition to the requirements at 2.6 above employees should also use common sense when choosing passwords and must avoid passwords that are easy to crack. For example choices such as "password", "password 1" and Pa$$w0rd" are equally unacceptable from a security perspective

2.8 A password should be unique, with meaning only to the employee who chooses it. That means dictionary words, common phrases and even names should be avoided. One recommended method to choosing a strong password that is still easy to remember: Pick a phrase, take its initials and replace some of those letters with numbers and other characters and mix up the capitalization. For example, the phrase "This may be one way to remember" can become "TmB0WTr!".

2.9 Employees must choose unique passwords for all of their company accounts and may not use a password that they are already using for a personal account.

2.10 All passwords must be changed regularly, with the frequency varying based on the sensitivity of the account in question. This requirement will be enforced using software when possible.

2.11 If the security of a password is in doubt– for example, if it appears that an unauthorised person has logged in to the account — the password must be changed immediately.

2.12 Default passwords — such as those created for new employees when they start or those that protect new systems when they're initially set up — must be changed as quickly as possible.

2.13 Employees may never share their passwords with anyone else in the company, including co-workers, managers, administrative assistants, IT staff members, etc. Everyone who needs access to a system will be given their own unique password.

2.14 Employees may never share their passwords with any outside parties, including those claiming to be representatives of a business partner with a legitimate need to access a system.

2.15 Employees should take steps to avoid phishing scams and other attempts by hackers to steal passwords and other sensitive information. All employees will receive training on how to recognise these attacks.

2.16 Employees must refrain from writing passwords down and keeping them at their workstations. See above for advice on creating memorable but secure passwords.

77 Elmers End Road, London, SE20 7UU . Tel: 020 8778 6111 . Fax 0208 778 5060 . Email: general@ddclimited.com

2.17 Employees may not use password managers or other tools to help store and remember passwords without IT's permission.

3. Systems and data security

3.1 You should not delete, destroy, or modify existing systems, programmes, 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 Office Manager. Downloading unauthorised software may interfere with our systems and may introduce viruses or other malware.

3.3 You must not attach any device or equipment including mobile phones, tablet computers or USB storage devices to our systems without authorisation from the Office Manager.

3.4 We monitor all emails passing through our system for viruses. You should exercise particular caution when opening unsolicited e-mails from unknown sources. If an email looks suspicious do not rely to it, open any attachments or click any links in it.

3.5 Inform the Office Manager immediately if you suspect your computer may have a virus.

4. Email

4.1 This policy applies to all staff, contractors and DDC Ltd who use the company email system. It applies no matter where that email use takes place i.e. on company premises, while travelling for work or whilst working from home. It also applies to the use of company email on any device whether owned by the employee or the company.

4.2 DDC Ltd makes email available to its employees where relevant and useful for their jobs. This email use policy describes the rules governing email use at the company. It also sets out how staff members are expected to behave when using email.

4.3 Email is a standard way to communicate in business. It is used widely and is arguable just as important as the telephone. As with any technology, email can cause difficulties if used incorrectly or inappropriate. This email policy:

- Reduces the security and business risks faced by DDC Ltd;

77 Elmers End Road, London, SE20 7UU . Tel: 020 8778 6111 . Fax 0208 778 5060 . Email: general@ddclimited.com

- Advised staff as to how they are permitted to use company email;
- Ensures employees follow good email etiquette;
- Helps the company satisfy its legal obligations regarding email use.

4.4 Staff members may use business email to communicate with customers or suppliers, market the company's products or distribute information to colleagues.

4.5 Only people who have been authorised to use email at DDC Ltd may do so. Authorisation is typically granted when a new employee joins the company and is assigned their login details for the company IT systems.

4.6 Unauthorised use of the company's email system is prohibited.

4.7 Users of the company email system must not:

- Open email attachments from unknown sources;
- Disable security or email scanning software;
- Send confidential company data via email. The IT department can advise on appropriate tools to use instead;
- Access another user's company email account. If they require access to a specific email, for example, if somebody is off sick, they should approach the Office Manager or the IT department;
- Use company email to share any copyrighted software, media or other materials owned by third parties unless permitted by that third party;
- Use the company's email system to perform any task that may involve a breach of copyright law and keep in mind that the copyright on letters, files and other documents attached to emails may be owned by the email sender or a third party. Forwarding such emails may breach this copyright.
- Staff members must always consider the security of the company's systems and data when using email.
- Users should note that email is not inherently secure. Most emails transmitted over the internet are sent in plain text. This means they are vulnerable to interception. Although such interceptions are rare, it is best to regard email as an open communication system and therefore not suitable for confidential messages and information.
- The company email system must not be used to send or store inappropriate content or materials and it is important that employees understand that viewing or distributing inappropriate content via email is not acceptable under any circumstances. Users must not:
- Write or send emails that may be defamatory or incur liability for the company;
- Create or distribute any inappropriate content or material via email. Inappropriate content includes; pornography, racial or religious slurs, gender-specific comments, information encouraging criminal skills or terrorism, or materials relating to cults, gambling and illegal drugs. This definition also covers any text, images or other media that could reasonably offend someone on the basis of a Protected Characteristic.

Any user who receives an email they consider to be inappropriate should report this to the Office Manager.

4.8 Users must be careful about making commitments or agreeing to purchases via email. An email message may be a legally binding contract between DDC Ltd and the recipient even if the user has not obtained proper authorisation within the company.

4.9 Users must not remove or change the standard company email disclaimer when they send messages

4.10 DDC Ltd may use email to market to existing and potential customers. There is sufficient legislation covering bulk email and the use of email for marketing. All email campaigns must be authorised by the marketing manager and implemented using the company's email marketing tool. Users must not send bulk emails using the standard business email system.

4.11 Email is often used to communicate with customers, partners and other important contacts. Although a relatively informal medium, staff should be aware that each email they send does affect the company's image and reputation.

4.12 Users must adopt a professional tone and observe appropriate etiquette when communicating with third parties by email and users must:

- Not forward on chain emails or 'humorous' messages;
- Always use a meaningful subject line rather than leaving it black or using a single word like 'hello';
- Only use the 'important message' setting sparingly for messages that are genuinely important;
- Never ask recipients to send a read receipt. Many people find these annoying and not all email services support them;
- Not use all capital letters in messages or subject lines as this can be perceived as impolite;
- Be sparing with group messages, only adding recipients who will find the message relevant and useful;
- Use the 'cc' (carbon copy) field sparingly. If someone needs to receive a message they should be included in the 'to' field;
- Use the 'bcc' (blind carbon copy) field to send group messages where appropriate as it stops an email recipient seeing who else was included in the email.

4.13 When using internal email users should consider the following:

- whether the issue would be better addressed via a face to face discussion or a telephone call.
- Whether email is the best way to send a document out for discussion as, often, it becomes very hard to keep track of feedback and versions

- ❖ It is usually unnecessary to 'reply to all'. Usually, it is better to reply and manually add others who need to see the message

5. Using the internet

5.1 Internet access is provided solely for business purposes. Occasional personal use may be permitted as set out in paragraph 6.

5.2 You should not access any web page or download any image or other file from the internet which could be regarded as illegal, offensive, in bad taste or immoral. Even web content that is legal in the UK may be in sufficient bad taste to fall within this prohibition.

5.3 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.

5.4 We may block or restrict access to some websites at our discretion

6. Personal use of our systems

6.1 We permit the incidental use of our systems to send personal emails, browse the internet and make personal telephone calls subject to certain conditions. Personal use is a privilege and not a right. It must not be overused or abused, and we may withdraw permission for it at any time or restrict access at our discretion.

6.2 The company recognises that email is an important tool in many people's daily lives and allows employees to use their company email account for personal reasons taking into account the following:

6.3 Personal email use should be of a reasonable level and restricted to non-working times e.g. breaks and during lunch;

6.4 All rules described in this policy apply equally to personal email uses. Inappropriate content is always inappropriate whether it is being sent or received for business or personal reasons.

6.5 Personal emails should be labelled "personal" in the subject header;

77 Elmers End Road, London, SE20 7UU . Tel: 020 8778 6111 . Fax 0208 778 5060 . Email: general@ddclimited.com

6.6 Personal emails must not affect your work or interfere with the business;

6.7 It must not commit us to any marginal costs;

6.8 Personal email use must not affect the email service available to other users e.g. sending exceptionally large files by email could slow access for other employees

6.9 Users may access their personal email accounts at work, if they are able to, via the company's email connection. For example, a member of staff may check their Google Mail or Hotmail during their lunch break.

7. Phone calls and text messages

7.1 Company mobile phones will be restricted to those members of staff who have direct responsibility for overseeing site works.

7.2 All new phones will be supplied with a shock resistant case and screen protector.

7.3 We will only have the facility to upgrade phones after a minimum period of 24 months and therefore the replacement of any mobile phone prior to this will result is a cost to the company. DDC will only accept responsibility for this cost where the replacement can be attributed to fair wear and tear. Where a phone requires replacement within 24 months as a result of physical damage that is not attributable to fair wear and tear then the company reserves a right to counter charge the individual phone user.

7.4 All new iPhones will have a 2GB monthly limit for data which should be sufficient for our company needs. The company reserves the right to counter charge the phone user should data usage exceed the 2GB monthly limit other than where the excess usage can be justified as a work expense.

7.5 On occasions where users are taking the mobile phone abroad then please contact the office for directions. Any costs incurred through incorrect usage whilst overseas will be counter charged to the user.

7.6 Personal calls should be kept to a minimum to minimise the disruption to both the productivity of yourself and site.

77 Elmers End Road, London, SE20 7UU . Tel: 020 8778 6111 . Fax 0208 778 5060 . Email: general@ddclimited.com

7.7 Failure to answer calls or listen to voicemails has resulted in missed appointments and disruption to projects/staff allocation. Please therefore respond in a timely manner to both calls and emails that relate to your work/job role.

7.8 Please check your phone at the end of each working day and where possible answer calls after this time if they are from the office or one of the manager's mobiles as this is likely to be relevant to the following day's schedule.

7.9 You are responsible for the phone receiving chargeable multimedia texts/results etc. Do not respond to any calls or messages that could be part of a scam.

7.10 Please notify the office immediately if the phone is receiving unusual messages.

8. Monitoring

8.1 Our systems enable us to monitor telephone, email, voicemail, internet and other communications. For business reasons, and in order to carry out legal obligations in our role as an employer, your use of our systems including the telephone and computer systems (including any personal use) may be continually monitored by automated software or otherwise.

8.2 We reserve the right to retrieve the contents of email 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):

- To monitor whether the use of the email system or the internet is legitimate and in accordance with this policy;
- To find lost messages or to retrieve messages lost due to computer failure;
- To assist in the investigation of alleged wrongdoing; or
- To comply with any legal obligation.

9. Prohibited use of our systems

9.1 Misuse or excessive personal use of our telephone or email system or inappropriate internet use will be dealt with under our Disciplinary Procedure. Misuse of the internet can in some cases be a criminal offence.

77 Elmers End Road, London, SE20 7UU . Tel: 020 8778 6111 . Fax 0208 778 5060 . Email: general@ddclimited.com

9.2 Creating, viewing, accessing, transmitting or downloading any of the following material will usually amount to gross misconduct (this list is not exhaustive):

- Pornographic material that is, writing, pictures, films and video clips of a sexually explicit or arousing nature);
- Offensive, obscene, or criminal material which is liable to cause embarrassment to us or our clients;
- A false and defamatory statement about any person or organisation;
- Material which is discriminatory, offensive, derogatory or may cause embarrassment to others (including material which breaches our Equal Opportunities Policy);
- Confidential information about us or any of our staff or clients (except as authorised in the proper performance of your duties);
- Unauthorised software;
- Any other statement which is likely to create any criminal or civil liability (for you or us); or
- Music or video files or other material in breach of copyright.

9.3 Employees, contractors and other users may also be held personally liable for violating this policy.

9.4 Where appropriate the company will involve the police or other law enforcement agencies in relation to breaches of this policy.

X pp R Kun — Signature

X OFFICE MANAGER — Job Title

X S. DAVIES — Name

X 26TH MAY 2022 — Date