3.3 Company Computer Policy

The Company regards its computer systems as a vital and integral part of its business. The Company expects their employees to use computers responsibly and only for the purposes of our business. We will treat seriously any actual, attempted or suspected infringement of this policy and may take disciplinary action, which could lead to dismissal in serious cases, against anyone acting or attempting to act in breach of this policy.

Regulation and Standards

1 Legislative Framework

England

- Regulation 22: Contact and access to communications
- Regulation 38: Storage of records, etc.
- Regulation 12: The protection of children standard

  http://www.legislation.gov.uk/uksi/2015/541/regulation/12/made
- General data protection rules (GDPR)

Wales

- Regulation 26: Safeguarding – overarching requirement
  https://www.legislation.gov.uk/wsi/2017/1264/regulation/26/made
- Regulation 27: Safeguarding policies and procedures
  https://www.legislation.gov.uk/wsi/2017/1264/regulation/27/made
- Regulation 48: Facilities and equipment
  https://www.legislation.gov.uk/wsi/2017/1264/regulation/48/made

Content;

1. Hardware

Rules regarding the use of hardware:

- No equipment must be moved without the consent of the person responsible for IT.
- No equipment must be attached to the network without the consent of the person responsible for IT.
- No equipment may be modified without the consent of the person responsible for IT.
- All equipment must be treated with due care and attention and maintained in a condition and environment conducive to good working order and long life. Any fault, loss or damage must

be reported to the person responsible for IT without delay. If in doubt consult the person responsible for IT.

- All equipment must be logged off correctly and powered down when not in use for long periods of time.
- Laptops must be kept secure when taken off site. Do not leave them unattended. All employees are required to take reasonable measures to minimise the risk of loss of Company data and software through theft. Particular care needs to be taken to ensure that laptops are not left unattended in vehicles or any other non-secure place.

2. Software

The computer will be set up by the person responsible for IT and must not be altered by the user.

You are only authorised to use systems and have access to information that is relevant to your job. You should neither seek information nor use systems outside these criteria. Unauthorised access to any of the Company's computers or network devices is a breach of this policy and will lead to disciplinary action.

Standard operating procedures must be followed at all times when using software. Where no procedures exist, consult your manager and follow any instructions given.

Under no circumstances may you purchase or load any software without approval from the person responsible for IT. This includes screen savers, wallpaper, downloads from the Internet and email attachments.

It is illegal to make copies of your software. Software issued by the Company for your use is licensed to the Company and is protected by copyright law. You must not make copies of software or distribute software that has been copied.

Storage media, such as external drives or CDs, which contain work related material, form part of the intellectual property of the Company and, because of the ease of portability of such sensitive commercial material, particular caution should be exercised when using, storing or transporting storage media whether within or outside the Company's premises.

3. Password Policy

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of the Company’s entire corporate network. As such, all employees are responsible for keeping their password secure.

4. Email

Your email address can receive emails from anyone connected to the Internet. You should limit the frequency of personal emails, which should be dealt with outside of normal office hours. You should ensure that your correspondents know that they should not send you “humorous” or illegal attachments such as pictures or executable programs. All external non-work related email messages should be deleted on receipt. Anyone found with offensive or pornographic material on his or her computer will be subject to immediate disciplinary action for gross misconduct. This will usually result in dismissal.

The Company reserves the right to access and monitor any or all areas of any computer and computer software systems which it owns (including email boxes and messages and telephone calls) from time to time for business reasons and training purposes. You should not therefore assume that any information held on the computer is private and confidential to you.

If you receive an email from an unknown source, or “junk” email you should delete this from your system immediately without opening it as it may contain a virus.

Emails may contain file attachments. These should not be opened unless they are received from a trusted source, i.e. from another known Company, employee or representative. If in doubt, forward the email to the IT department for verification.

Emails to commissioners, suppliers and other business contacts should be restricted to Company business. Confidential information about or relating to the business of the Company, its clients, suppliers or contacts should not be transmitted outside the Company via email unless done so in the course of business. Confidential information should not be left on display on an unattended workstation.

Regular housekeeping is required to delete unwanted emails to prevent the file server filling up.

You should be aware that deleted emails will remain held on the system for some time and will be accessible from back up if required for investigation of complaints of systems abuse.

You must not distribute sensitive commercial data concerning the Company to any external parties. Doing so will make you liable for disciplinary action for gross misconduct which may result in your dismissal.

5. Guidance for Appropriate Use

Email in its native form is a non-secure medium and care should be taken when composing, sending and storing messages. It is possible for messages not to be received at their intended destination or to be intercepted. If email services are used for business critical or sensitive communications, you must send and reply via Bryn Melyn Care’s encrypted email service (Egress)

Email should be regarded in the same way as any other business communication and should be treated as a Company record. You should adopt a style and content for emails, in particular those sent to external recipients that present a professional image. It is recommended that you adopt the same standards for email as for letters and memos, although the style may be more informal.

Confidential information about or relating to the business of the Company, its clients, prospects, suppliers or contacts should not be transmitted outside the Company via email unless done so in the course of business and sufficient steps are taken to safeguard security.

6. Inappropriate Use

Employees must not send internally or externally or obtain material (whether in the form of text or images) which is libellous or defamatory, illegal, obscene, sexually explicit, bullying, discriminatory or disparaging of others particularly in respect of their race, national origins, sex, sexual orientation, age, disability, religious or political beliefs.

Employees are reminded that material which they find acceptable, for example the content of email jokes or chain letters might be offensive to others. It is recommended that you take care and give sufficient thought to what you send. Messages can be misconstrued and should not become a substitute for "one-to-one" conversations. You should not send humorous material to business contacts. It can frequently be misunderstood or cause offence.

7. Internet Access

Internet access will be granted for business reasons only during working hours. Usage is limited to work related activities.

Anyone found visiting pornographic sites will be subject to immediate disciplinary action and if necessary the police will be informed. Anyone found downloading or circulating pornographic material or other non-business material will be subject to immediate disciplinary action and if necessary the police will be informed.
Please note that the main servers may maintain a record of Internet access by users and these will be monitored as necessary and results forwarded to line managers and the police, if appropriate.

8. Revision History

Date last updated: May 2020

Date of next review: May 2021

Date of release: December 2018

End