φύσις

Staff- computers and electronic communication

Physis Heathgates Academy

Review Date - October 2017

Staff - Computers & Electronic Communica,on

Index

1. Introduc,on

1.1 This policy document is intended only for the use of the employees of Physis Quantum and should be treated as confiden5al.

1.2 Distribu5on outside of Physis Quantum should only occur with the wriGen consent of the CEO.

1.3 All Physis Quantum employees are expected to read this policy and their understanding of this policy will be assessed during the Induc5on Process, regularly during Supervision, and during mandatory training events.

1.4 Employees will be expected to abide by and work within this policy framework at all 5mes, both during and aPer their employment, as s5pulated in their Contract of Employment.

1.5 This policy was last revised on 30.10.16. and it will be reviewed bi-annually and/or in accordance with changes in company structure, relevant legisla5on and guidance.

1.6. This policy is fully in accordance with the Staff Handbook.

2. Policy Statement

2.1. This policy sets out the Company's guidelines on access to and the use of the Company's computers and on electronic communica5ons.

2.2. It also sets out the ac5on which will be taken when breaches of the guidelines occur.

3. Guidance for Staff

3.1. You are only permiGed to use the Company's computer systems in accordance with the Company's Data Protec5on, Monitoring Policies and the following guidelines.

3.2. Your responsibili5es:

- The Company's computer systems and soPware and their contents belong to the Company and they are intended for business purposes only.
- You are not permiGed to use the Company's systems for personal use, unless authorised to do so by your manager.
- You are not permiGed to download or install anything from external sources unless you have express authorisa5on from your manager.
- No device or equipment should be aGached to the Company's systems without the prior approval of your manager.
- The Company has the right to monitor and access all aspects of its systems - including data that is stored on the Company's computer systems in compliance with the Data Protec5on Act 1998.

3.3. System Security

- You must only log on to the Company's computer systems using your own password which must be kept secret. You should select a password that is not easily broken (e.g. not your surname).
- You are not permiGed to use another employee's password to log on to the computer system, whether or not you have that employee's permission.
- If you log on to the computer using another employee's password, you may be liable to disciplinary ac5on up to and including summary dismissal for gross misconduct.
- If you disclose your password to another employee, you may also be liable to disciplinary ac5on.

- To safeguard the Company's computer systems from viruses, you should take care when opening documents or communica5ons from unknown origins.
- AGachments may be blocked if they are deemed to be poten5ally harmful to the Company's systems.
- All informa5on, documents, and data created, saved or maintained on the Company's computer system remains at all 5mes the property of the Company.

3.4. Use of e-mail

- Where the Company's computer systems contain an e-mail facility, you should use that e-mail system for business purposes only.
- E-mails should be wriGen in accordance with the standards of any other form of wriGen communica5on and the content and language used in the message must be consistent with best prac5ce. Messages should be concise and directed to relevant individuals on a need to know basis.
- You should take care when opening e-mails from unknown external sources. AGachments to e-mails may be blocked if they are deemed to be poten5ally harmful to the Company's systems.
- E-mails can be the subject of legal ac5on (for example, claims of defama5on, breach of confiden5ality or breach of contract) against both the employee who sent them or the Company.
- As e-mail messages may be disclosed to any person men5oned in them, you must always ensure that the content of the e-mail is appropriate.
- Abusive, obscene, discriminatory, harassing, derogatory or defamatory e-mails must never be sent to anyone. If you do so, you may be liable to disciplinary ac5on up to and including dismissal without no5ce.

3.5. Internet access

- You are required to limit your use of the internet to sites and searches appropriate to your job.
- The Company may monitor all internet use by employees.

- You are expressly forbidden from accessing web pages or files downloaded from the internet that could in any way be regarded as illegal, offensive, in bad taste or immoral.

3.7. Monitoring

Monitoring of the Company's computer systems and electronic communica5ons may take place in accordance with the Company's Monitoring Policy. Please refer to the Company's Monitoring Policy for further details.

3.8. Misuse of Computer Systems

3.8.1. Examples of misuse include, but are not limited to, the following:

- Accessing on-line chat rooms, blogs, and social network sites.
- Use of on-line auc5on sites.
- Sending, receiving, downloading, displaying or dissemina5ng material that discriminates against, degrades, insults, causes offence to or harasses others.
- Accessing pornographic or other inappropriate or unlawful materials.
- Engaging in on-line gambling.
- Forwarding electronic chain leGers or similar material.
- Downloading or dissemina5ng copyright materials.
- Issuing false or defamatory statements about any person or organisa5on via the Company's electronic systems.
- Unauthorised sharing of confiden5al informa5on about the Company or any person or organisa5on connected to the Company.
- Loading or running unauthorised games or soPware.

3.8.2. Any evidence of misuse may result in disciplinary ac5on up to and including dismissal without no5ce. If necessary, informa5on gathered in connec5on with the inves5ga5on may be handed to the police.

3.9. Security of Informa,on when Removed from Company Premises.

3.9.1. All computers including laptops must be password protected at all 5mes and any device whatsoever (including hard drives and pen drives, etc) must be encrypted at all 5mes when any company informa5on of any kind is contained on that device.

3.9.2. All members of staff should remain constantly vigilant in regard to the safety and security of any and all informa5on regarding the company, its clients and employees.

3.9.3. No informa5on regarding the company, its clients or employees should ever be removed from the work environment without the express permission of the relevant line manager.

3.9.4. The establishment of a clear plan for the safe transit and storage of any informa5on to be taken outside of company premises must be established, agreed and complied with. Failure to do so is likely to cons5tute a disciplinary maGer.

3.10. Complaints of bullying and harassment

If a member of staff believes that they have been harassed, bullied or are offended by material received from a colleague, you should inform your line manager immediately.