Finance and Resources Committee, 10 September 2013

Information Technology Policy 2013

Executive summary and recommendations

Introduction

This paper sets out the revised Information Technology policy (IT policy).

Decision

The Committee is asked to discuss and agree the policy.

Background information

The IT policy has been updated to reflect the information technology and services that are now being used at the HCPC. It sets out more clearly the acceptable use of the HCPC Information Systems enabling compliance with legislative obligations. The scope of the policy has also been extended to include council members, Partners and contractors as well as employees.

The policy has been created following a document review of the related policies for six of the other health and care regulators in the UK as well as a legal review by the HCPC lawyers. The policy went through the process of employee consultation in August.

Resource implications

There are no resource implications.

Financial implications

There are no financial implications.

Appendices

Appendix 1- Information Technology Policy.

Date of paper

8 August 2013.

Information Technology Policy

First published in September 2013

Guy Gaskins Director of Information Technology

Contents

1. Introduction

1.1. The Health and Care Professions Council (HCPC) creates, collects and manages information and data in the execution of its duties as a regulator of health, psychological and social care professions.

1.2. The information and data will include personal and sensitive information that is protected by the Data Protection Act 1998, other applicable law and by the HCPC confidentiality policy.

1.3. The HCPC uses electronic information and communication systems and related equipment (HCPC Information Systems) to support the management of the information and data.

1.4. Inappropriate or unacceptable use of the HCPC Information Systems may result in legal claims against both the HCPC and individual users.

2. Purpose

2.1. The Information Technology policy (IT policy) sets out the acceptable use of the HCPC Information Systems as well as the behaviour expected from the people who use those systems. In this policy the terms ‘you’ and ‘your’ refer to any such person or user of the HCPC Information Systems.

2.2. The objective of the IT policy is to ensure that the people who use the HCPC Information Systems to manage the information and data do so in a way that maintains the following attributes of the systems and information:

2.2.1. Confidentiality: preventing the unauthorised use or disclosure of information;

2.2.2. Integrity: safeguarding the accuracy and trustworthiness of information and systems; and

2.2.3. Availability: ensuring reliable access to the information and resources when you need it.

2.3. The HCPC encourages appropriate use of the HCPC Information Systems where it supports the goals and objectives of the HCPC.

3. Scope

3.1. This policy applies to all those persons accessing the HCPC Information Systems. It applies to all HCPC employees and to:

3.1.1. council and committee members;

3.1.2. contractors;

3.1.3. Partners; and

3.1.4. anyone given temporary access to and use of the HCPC Information Systems including temporary agency workers.

3.2. Any person that has access to the HCPC Information Systems as part of a contractual support, maintenance, development or service agreement will be bound by the terms and conditions of that contract.

3.3. The policy applies to all locations from which you access the HCPC Information Systems including remote access using a VPN (virtual private network) or similar technology.

3.4. The HCPC Information Systems refer to and include all aspects of information technology, both hardware and software including any HCPC extranet, to which access has been granted or which has been provided by the HCPC.

3.5. The HCPC Information Systems includes but is not limited to the following services, technology and systems:

3.5.1. corporate email;

3.5.2. internet connectivity;

3.5.3. desktop and mobile telephony including smart phones;

3.5.4. personal computers;

3.5.5. the network including Wi-Fi;

3.5.6. electronic storage including flash drives;

3.5.7. business applications such as the registration system and case management system; and

3.5.8. printers, copiers and scanners.

4. Legislation

4.1. This policy reflects obligations which are imposed upon HCPC by law and which are relevant to the provision and use of information technology, systems and data. These include but are not limited to:

4.1.1. Computer Misuse Act 1990;

4.1.2. Copyright, Designs and Patents Act 1988;

4.1.3. The Data Protection Act 1998;

4.1.4. Freedom of Information Act 2000;

4.1.5. Human Rights Act 1998;

4.1.6. Regulation of Investigatory Powers Act 2000; and

4.1.7. Telecommunications (Lawful Business Practice) (Interception of Communications) Regulation 2000.

5. HCPC Policies

5.1. There are a number of HCPC policies that this policy directly relates to.

For employees these and all policies can be found in the Employee Handbook which is available to all employees online or by request to the HR department. These include but are not limited to:

5.1.1. Capability procedure;

5.1.2. Code of Conduct and Behaviour;

5.1.3. Confidentiality;

5.1.4. Disciplinary and Dismissal Policy and Procedure;

5.1.5. Office Security Policy;

5.1.6. Social Media Policy; and

5.1.7. Working from home.

For Council members the relevant policies are available on the HCPC members extranet and from the Secretariat and include but are not limited to:

5.1.8. Code of Conduct for council and committee members.

For HCPC Partners the relevant policies are available in the online Partner Handbook and on request from the Partner department and include but are not limited to:

5.1.9. Partner Code of conduct; and

5.1.10. Partner Complaints procedure

6. Principles

6.1. When using the HCPC Information Systems you are required to maintain standards of honesty and integrity at all times in a manner reasonably expected of anyone working for or on behalf of a reputable organisation and as outlined in the Code of Conduct and Behaviour.

6.2. You should immediately disclose any misuse of the HCPC Information Systems to your manager, the Director of IT or to the HR department.

6.3. The HCPC will monitor your use of the HCPC Information Systems and will take action in respect of breaches of the policy. A breach of this policy is likely to be regarded as:

6.3.1. An act of misconduct or gross misconduct by an employee. Where an employee has breached this policy the Disciplinary and Dismissal Policy will apply.

6.3.2. A breach of the Code of Conduct for council and committee members.

6.3.3. A breach of the Partner Code of Conduct for HCPC partners which may result in termination of the partner agreement.

6.3.4. An act of misconduct or gross misconduct for a contractor. This may result in the termination of any relevant contract and may also result in further legal action being taken.

6.4. You may only access the HCPC Information Systems if you have been authorised to do so and your use of those systems must comply with this IT Policy, which may be revised from time to time and is available on the HCPC Intranet and from the IT department.

7. Ownership of IT Information Systems

7.1. The HCPC Information Systems including all software are owned, licensed or procured by the HCPC and you must use them exclusively for the benefit of the HCPC in connection with its business.

7.2. All data, files or information that you create on, store on or transmit by and through the HCPC Systems, including word processing files, emails, voicemail messages, database files etc. are and remain the sole property of the HCPC. Nothing that you enter, retain or transmit is or shall be deemed to be your personal property.

7.3. You must not procure any IT Information System on behalf of the HCPC including third party services, hardware and software irrespective of whether the service is delivered internally by the IT department or externally by a third party service provider unless you have received written authorised by the IT department.

8. Copyright

8.1. You may not use the HCPC Information Systems in ways that infringe any party's copyright or related rights. Violations of copyright or other similar rights may subject you and the HCPC to legal liability.

8.2. Materials in websites or other external systems, via removable media such as flash drives or email messages and attachments that you receive, may contain intellectual property belonging to others (including copyright, trade secrets or trademarked information).

8.3. You must not download, store, copy, publish or distribute material that is controlled through copyright or by license; this includes programs, screensavers, graphics, files, art, photographs, video files and music files. unless:

8.3.1. You have the express authorisation from the copyright owner or licensor; or

8.3.2. You are otherwise permitted by copyright law to copy the work in that manner.

8.4. You must not use materials or content for which the HCPC owns the copyright other than where it is necessary to fulfil your role or responsibilities for or on behalf of the HCPC.

9. Access

9.1. You are granted access to the HCPC Information Systems on the condition that all of the terms and conditions of the Information Technology Policy are adhered to.

9.2. Access to the HCPC Information Systems is granted in accordance with and to support your specific role or responsibilities for or on behalf of the HCPC.

9.2.1. You must not attempt to gain access to those parts of the HCPC Information Systems, information, files or data that you have not been granted explicit access to.

The Computer Misuse Act makes unauthorised access to, or modification (including deletion) of, computer held software or data a criminal offence.

9.2.2. You may be granted access, in connection with your role or responsibilities, to information, documents and materials that have been generated by the HCPC or received from third parties.

If you are granted such access, you must keep the information fully confidential.

9.3. The HCPC, at its sole discretion, may provide you with access to the internet by way of the HCPC Information Systems. The HCPC may withdraw access to the internet, block or restrict your access to websites or internet services including the ability to receive from or send to specific email addresses at its sole discretion.

10. Security

10.1. You are responsible for the security and use of the equipment allocated for your use including desktop computers, laptops, desk phones, mobile phones, flash drives etc. You must take reasonable measures to protect it from loss or, damage and to keep it in good working order.

10.2. If you leave a device unattended such as a desktop PC, laptop or mobile telephone, you should log off or lock your device to prevent unauthorised users accessing it in your absence.

You are responsible for all activity performed under your unique username or account.

10.3. All data and information that you transfer out of the HCPC and is either protected under the Data Protection Act 1998 or is sensitive to the operation of

the HCPC must be securely encrypted before transfer. This includes transfer by email, flash disk, internet upload, DVD, CD etc.

Examples of personal data and sensitive information would include lists of names and addresses, and private committee papers respectively.

Guidance for encrypting files is available on the HCPC intranet and by request to the IT department.

10.4. You must not download or install software programmes into the HCPC Information Systems without written authorisation from the IT department.

10.5. You must not deliberately introduce into the HCPC Information Systems computer viruses or malicious software including Trojan horses, worms etc.

10.6. Passwords

You will be required to create and use several passwords to gain access to different services of the HCPC Information Systems for example as part of a network logon, email account, HR system logon, purchase order system logon etc.

10.6.1. You must never disclose passwords to anybody else. This includes disclosing to the IT team unless your password is consequentially and immediately reset.

10.6.2. You must never write down the passwords that you use.

10.6.3. Your passwords should be complex. Guidance for creating complex and memorable passwords is available on the HCPC intranet and by request to the IT department.

10.7. Use of private devices

You may use a non-HCPC Information System from time to time to process HCPC documents, data and files etc but only:

10.7.1. When no other viable method of using an HCPC Information System is available, for example where a HCPC laptop has malfunctioned and cannot connect remotely to the HCPC infrastructure and no other appropriate HCPC device is available. Or

10.7.2. Where the HCPC does not provide HCPC Information Systems to fulfil your role or responsibilities for or on behalf of the HCPC for example council members reviewing electronic versions of private council papers.

In all cases:

10.7.3. You remain responsible for the security of the documents, data and files etc. that are accessed from time to time using non-HCPC Information Systems such as a private computer.

10.7.4. You are responsible for ensuring that the non-HCPC Information Systems have adequate protection against malicious software and unauthorised access.

10.7.5. You should immediately remove HCPC documents, data and files etc. from any non-HCPC Information Systems when there is no longer a valid and reasonable need to access them.

10.8. You must report immediately any actual or suspected breach of IT security including:

10.8.1. loss of mobile devices such as laptops, mobile phones, flash storage drives etc;

10.8.2. introduction of a virus or malicious software;

10.8.3. disclosure of a password to anybody else;

10.8.4. personal or sensitive data loss outside of the HCPC physical and technical environment;

10.8.5. actual or attempted unauthorised access to HCPC Information Systems; and

10.8.6. any activity that you suspect is illegal.

11. Monitoring

11.1. The HCPC continually monitors the use of the HCPC Information Systems including any personal use, for business reasons and in order to perform various legal obligations in connection with its functions.

11.2. Monitoring is only carried out to the extent permitted by law.

11.3. The HCPC will monitor your use of the HCPC Information Systems including the telephony system for specific reasons. These include but are not limited to:

11.3.1. ensure that the use of the HCPC Information Systems including the email system, telephony system or internet is legitimate and in accordance with this and other policies;

11.3.2. ascertain correct and acceptable service standards are being maintained;

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

11.3.4. ensure compliance with regulatory requirements and practices and procedures relevant to the business of the HCPC;

11.3.5. ensure that the HCPC Information Systems are operating effectively;

11.3.6. assist in the investigation of wrongful acts; and

11.3.7. comply with any legal obligation including the prevention or detection of crime and subject access or freedom of information requests.

11.4. By your use of the HCPC Information Systems, you acknowledge that the HCPC can and does examine logs of your activity on the HCPC Information Systems.

11.5. The HCPC reserves the right to access at any time any computer file, data file, log file, document, voicemail message, instant message, email message or mailbox to maintain and protect the HCPC Information Systems for the benefit of the HCPC.

11.6. Personal information collected through monitoring will not be used for purposes other than that for which the monitoring was introduced unless it is in your interest to do so or it reveals activity that an employer could not reasonably be expected to disregard.

12. Personal Use

12.1. Your personal use of the HCPC Information Systems at any time is a privilege. The HCPC reserves the right to withdraw permission for personal use at any time.

12.2. Your personal use should not interfere with the performance of your responsibilities; it should be infrequent, short in nature and lawful.

12.3. The act of your personal use should not cause distress or upset to anyone likely to view, hear or become aware of its content.

12.4. Your personal use of the HCPC Information Systems should be appropriate for that of a public regulator, no activity should reflect unfavourably upon the reputation of the HCPC.

12.5. If you identify yourself as working or acting for the HCPC you should ensure that content associated with you is consistent with your role in the organisation and does not compromise the reputation of the HCPC.

12.6. You may use the HCPC Information Systems for personal use in the following circumstances:

12.6.1. to access the internet including using authorised web based email service providers such as Google mail and Hotmail where it does not contravene any other HCPC policy;

12.6.2. to make and receive personal telephone calls using desk and mobile phones; and

12.6.3. to access the internet by using your personal equipment to connect to an authorised HCPC Wi-Fi network designated either for public use or for employee's personal use. You are not permitted to connect your personal equipment to any other HCPC network.

12.7. All calls made on the HCPC's telephone systems, including mobiles, are itemised. You may be charged for personal calls, text messaging and data use that is reasonably identified as excessive.

12.8. You are not permitted to use the corporate email services for personal use. Any and all emails sent from or received by the corporate email system including by mobile phone or mobile device will be considered to be a business communication and may be intercepted, opened, read, deleted, archived and disclosed in legal proceedings in the same way as paper documents by the HCPC.

12.9. You are not permitted to use HCPC storage on HCPC Information Systems for your personal data or information including files, pictures, music, programs, messages, and video or voice recordings.

12.10. You are not permitted to connect personal equipment directly to the HCPC Information Systems including non-HCPC mobile phones, USB flash drives and laptops without written permission from the IT department.

12.11. Methods of protection employed by the HCPC in order to maintain the integrity of the HCPC Information Systems may adversely affect the functioning of any non-HCPC device directly connected to the HCPC Information Systems, causing them to be temporarily or permanently disabled.

13. Unacceptable behaviour

13.1. The following list identifies a number of activities that are unacceptable and would be considered a breach of this policy. The list is not exhaustive and only identifies examples of unacceptable use whether as part of day to day duties or as part of personal use:

13.1.1. Supporting any business other than the HCPC including but not limited to any form of solicitation or advertising.

13.1.2. Using the HCPC Information Systems in any way as part of a private business.

13.1.3. Any activity that takes a disproportionate amount of your time or concentration away from the normal responsibilities on behalf of the HCPC, for example regular and prolonged use of non-work related websites during working hours including sports, entertainment, gaming sites, etc.

13.1.4. Harassment, including but not limited to: threats; statements of intimidation; derogatory comments including comments or messages relating to a person's religion and belief, race, gender, age, sexual orientation, gender reassignment, marriage and civil partnership, pregnancy and maternity or disability.

13.1.5. Impersonation of an individual to gain increased privileges such as access to data, services or authority including the ability to authorise purchases etc.

13.1.6. Sending unsolicited electronic messages such as email, including the sending of 'junk mail' or 'chain letters' to recipients who have not specifically requested the communication.

13.1.7. Any activity that causes the impedance of, disruption to or loss of access to an HCPC Information System including the interception of network traffic.

13.1.8. The transport of personal or sensitive data outside of the HCPC Information Systems in an unencrypted format.

13.1.9. Accessing pornographic material (including writings, pictures, films, or video clips of a sexually explicit nature).

13.1.10. Accessing offensive, obscene or criminal material or material which is likely to cause embarrassment to the HCPC or any person associated with the HCPC

13.1.11. Making false and defamatory statements about any person or organization.

13.1.12. Distributing without authorisation confidential information about the HCPC or any person associated with the HCPC.

13.1.13. Making any statement which is likely to expose you, the HCPC or any person associated with the HCPC to criminal or civil liability.

13.1.14. Material breach of copyright.

13.1.15. Engaging in online gambling.

13.1.16. Disabling or circumventing security controls such as anti-virus software, monitoring services, firewalls, USB port protection etc.

14. Agreement

I confirm that I have been granted access to the HCPC Information Systems for the purpose of my role and I confirm that I understand and agree to comply with the terms of this policy which may be revised from time to time.

Name:…….

Signature:……...

Date:……..