Doc. Ref:	IT - AUP
Issue:	1
Amended:	27/09/2016
Review date:	September 2017

Acceptable Usage Policies

IT – Acceptable usage

If printed then this document is uncontrolled and for reference purposes only; always check the intranet for the latest version

Contents

1. Introduction

The use of IT equipment and services is an essential tool for PCH and its staff to deliver effective services and support the organisation in achieving its aims and objectives.

It is important that any use of IT equipment and services is used in an appropriate way allowing for the flexibility and needs of the organisation and staff whilst meetings its obligation to data security and the protection of information.

This document outlines 'acceptable usage' for various aspects of IT equipment and services and is in addition to specific 'Codes of Practice' that you may be asked to sign depending on the equipment you have been issued with and the department you work for.

The information contained within this document is also easily accessed via the IT department site on the PCH Intranet.

2. Use of IT within PCH

PCH adopts a flexible approach to the use of various technologies and services. There is a balance between flexibility and use of equipment (supporting staff to do their job) versus the need for security and protection of personal and corporate data (files, documents and information).

PCH IT allows for the use of various devices, platforms and applications to meet the requirements and demands of the organisation and to enable staff to use appropriate equipment to access information and services (as and when needed) to deliver effective services.

The use of corporately issued equipment/hardware AND personally owned equipment (phones, tablets, home PCs) are permitted provided staff follow the 'acceptable usage' policies outlined in this document.

3. Use of IT Equipment

PCH makes available various types of equipment to enable staff to fulfil their duties. This sections covers 'acceptable usage policy' for core IT equipment.

3.1. IT Usage

General guidance	
	A number of general rules, guidelines and recommendations apply to the use of IT within PCH. Most of these are common sense and practical aimed at allowing staff to do their job whilst being mindful of security and protection of data.
	If in doubt or you have any questions or queries or require any advice please contact the IT Service Desk (ext. 8118).

Do	Do Not
System & Network Security	
Change your password immediately if you suspect that it may have become known by any other person	Do not send confidential information via external/personal e-mail accounts or electronic media without management authorisation and without protecting it appropriately (if in doubt please contact IT Service Desk
Inform the IT team immediately if anyone asks you to reveal your password	Never share or divulge your password with anyone
Change your password regularly (as prompted) and avoid using obvious or standard passwords	Never attempt to access systems, application or files to which you are not authorised
Protection from Viruses and Malware	
Always report any potential 'infections' or attacks to the IT Service Desk IMMEDIATELY	Do not open any untrusted or unexpected emails, attachments or web links – if in doubt contact IT Service Desk for advice
Always use up to date virus checking software to ensure no infections are present on any media received from outside PCH	Do not download/install software without consent from IT
	Do not circumvent any existing protection – switching off virus protection or bypassing PCH firewall (security gate)
Protecting the Organisations Reputation	
Use PCH standard format for email signature and 'out of office' messages	Do not express personal views or represent the organisation without management approval
Be aware that PCH web and email usage is actively monitored (inappropriate use will be dealt with via the PCH disciplinary policy)	Do not use or violate 'copyright' protected information or material (including media, software and information)
	Do not access, view or distribute objectionable material or information (i.e. pornographic, racist, terrorism)
	Do not use systems or send emails that discriminate on the basis of race, sex or other biases
Service Levels	
Avoid, wherever possible, using excessive system resources during peak working hours. An example would be transferring large files between 9 a.m. and 5 p.m. Please contact IT Service Desk for further guidance	Avoid any unnecessary 'CC' or 'BCC' in emails. This causes duplication and unnecessary work
Move important email messages that you want to keep for reference to an appropriate area of the network storage or SharePoint and/or archive your emails regularly to the email archive folder to avoid the build-up of unnecessary emails (recommend deleting or achieving every 3 months as a minimum)	Do not use PCH time or IT equipment for personal use or business matters not related to PCH unless agreed with your manager and then only in a trustworthy way. IT systems are monitored and abuse will be deal with on an individual basis under existing PCH disciplinary procedures
When sharing information (particularly via email) use 'links' to data/documents and avoid sending attachments wherever possible	

If in doubt or if you have any concerns or queries please contact the IT Service deck (ext 8118)

3.2. Use of Mobile Devices (Phones, Tablets)

PCH uses a number of different mobile devices to enable staff to fulfil their job role. PCH also welcomes the opportunity for staff to use their own mobile devices for work purposes where appropriate.

Mobile devices as defined as a device capable of receiving mobile calls and/or able to access and display corporate information (documents, data and applications). This typically included mobile phones, phablets, tablets and sim enabled laptops/notebooks.

3.2.1. Corporate Mobile Devices

General guidance	
	Once you have been authorised as a mobile phone user, you will be allocated a mobile device, SIM card, battery charger, protective case and a copy of the mobile 'code of practice'. This equipment will remain your responsibility until such time as it is returned and signed for. The mobile number will be allocated to you as long as you need the mobile device to do your job.
	Corporate mobile devices are provided for use in connection with the business of PCH. Personal calls and SMS Texts are permitted within reason. However calls abroad or to premium numbers (e.g. 0898, 0906) are strictly prohibited for personal use
	All corporately issued devices (and peripherals) must be returned if you are leaving employment of PCH.

Do	Do Not
Mobile Device Usage	
Contact the IT Service Desk in the event of any equipment failure or breakages	Whilst there are times when it may be acceptable to make or receive short personal calls or messages, for instance during emergencies, the misuse of company time will leave employees potentially liable to disciplinary action
Do use your mobile devices for taking photographic evidence provided it is line with your work AND that permission is sought if photo content involves a 3rd party (e.g. another person or personal property)	Do not download or install applications (from Apple, Google and vendor apps store) that will breach copyright of licensing infringements. If in doubt contact IT Service Desk
If prompted to upgrade phone/tablet apps do so when connected to WiFi (e.g. Plumer Guest) to avoid any unnecessary breach of data allowance	Do not use mobile phones whilst driving. Drivers should make and receive calls in the vehicle only when stationary and parked in a safe place with the engine switched off Drivers of vehicles fitted with in car or speaker systems must park safely when making or receiving calls. Device features such as GPS or Maps should not be used whilst driving
Security and protection of data/information	
Be aware that PCH mobile phone call/data usage is actively monitored (inappropriate use will be dealt with via the PCH disciplinary policy)	Do not divulge or share your mobile device PIN code with anyone (4 digit PIN code is enforced for all corporate mobile device)
Be aware that PCH web and email usage is actively monitored (inappropriate use will be dealt with via the PCH disciplinary policy)	Do not leave any corporately issued equipment left unattended. This applies in and out of the office
	Do not leave phones in an unattended vehicle. This includes cars parked in any car park, place of work, in your garage or on your driveway. Phones must not be left in the boot or glove box of your vehicle under any circumstances
	When using mobile devices do not express personal views or represent the organisation without management approval
	Do not use or violate 'copyright' protected information or material (including media, software and information)
	Do not access, view or distribute objectionable material or information (i.e. pornographic, racist, terrorism)
Loss / safe keeping of equipment	
Immediately notify the IT Service Desk if equipment is lost or stolen If you have a O2 mobile you can ring 901 direct to bar the lost phone yourself. Failure to bar a phone that is known to be lost will result in PCH being charged for any unauthorised calls made and these will, in turn, be recharged to the appropriate department	Do not subject or expose your mobile device to situations or adverse conditions that may cause or result in damage (i.e. water, heat)
Be aware that PCH web and email usage is actively monitored (inappropriate use will be dealt with via the PCH disciplinary policy)	

3.2.2. Use Your Own Device (BYOD/UYOD)

General guidance	
	PCH welcomes enquiries from staff to you their own mobile device. PCH IT have arrangements in place that enables staff to use their mobile phones, phablets and tablets in an isolated (separate) way to personal usage. This ensures that corporate data is not compromised and not shared with the personal aspects and features of your mobile device.
	Using PCH mobile device management software ensures that corporate data can be protected and allows you the freedom to access and use corporate services and data on your own device.
	As a result of using your own device there will be no added expectations for you to carry out additional work or check work emails outside of my normal working hours. Any work carried out will, unless otherwise agreed with management, be your choice and unpaid.

Do	Do Not
Mobile Device Usage	
Do use your mobile devices for taking photographic evidence provided it is line with your work AND that permission is sought if photo content involves a 3rd party (e.g. another person or personal property)	No reimbursement for business calls made on personally owned mobile devices will be made to employees other than in exceptional circumstances
	No reimbursement for any breach of personal tariff (voice or data) due to corporate use of personal device
Security and protection of data/information	
Where a personal mobile device is being used it must adhere to PCH security terms and conditions. In its simplest form, the mobile device must be secured with a PIN or Password. Device should be enrolled in the corporate MaaS360 (Mobile Device Management) software unless agreed by PCH Management	Do not divulge or share your mobile device PIN code with anyone
	Do not attempt to uninstall PCH device control software (MaaS360). If you no longer wish to use your own device for business purposes please contact the IT Service Desk
Loss / safe keeping of equipment	
Immediately notify the IT Service Desk if equipment is lost or stolen PCH IT can lock and remotely delete any corporate data held on your personal device using remotely control mobile device management software (MaaS360)	PCH is not responsible and will not reimburse any loss or damage arising from the use of personal devices for corporate purposes (e.g. lost or stolen)

4. Use of Web based services

The use of web based services (internet, email and social media) is embedded in daily tasks, actions and activities of staff and provides access to core services and information.

However, we need to be mindful that web based services are externally hosted and managed which introduces additional risks in how we access, use and manage information/data.

Typically this involves the use the internet, email, social media and Plumer House guest Wi-Fi facility.

4.1. Internet

General guidance	
	Staff are expected to use the Internet responsibly and productively. Internet access is limited to job-related activities during working time only and personal use is only permitted outside working time (e.g. outside core hours, lunch breaks)
	PCH also recognises that the internet is embedded in many people's daily lives. As such, it allows employees to use the internet for personal reasons provided that it is used outside working time (e.g. outside working/core hours, lunch breaks)
	If you are unsure about what constitutes acceptable Internet usage ask your supervisor/manager for further guidance and clarification
	Internet usage is monitored
	Staff must always consider the security of the company's systems and data when using the internet. If required, help and guidance is available from your line manager or the IT Service Desk
	Certain internet sites and content are filtered and/or restricted to protect the organisation and staff risks and an unsuitable information/pictures

Do	Do Not
Internet Usage	
Use the intranet to access work related information, research and tasks	Do not use / access internet during working time for non work related tasks, actions or information
Security and protection of data/information	
If you use non corporate issued equipment or use your own equipment to access the internet for business purposes make sure virus protection is switched on and up to date	Do not use or violate 'copyright' protected information or material (including media, software and information)
If you think you have been attacked or the source of any potential virus or malware notify the IT Service Desk immediately	Do not click on/open links that are unprompted and/or unexpected and not related to your task. This could lead to ransomware and malware infections!
Protecting the Organisations Reputation	
	Do not use the internet for sending or posting discriminatory, harassing, or threatening messages or images
	Do not use the internet for sending/stating personal views, comments or opinions

4.2. Email

General guidance	
	The organisations email system is provided for legitimate business purposes only.
	Under no circumstances should you use your PCH email system for personal use

Do	Do Not
Email Usage	
Use the organisation Email systems for business related matters	Do not click on any downloads links or install any software via Email. If have a requirement contact the IT Service Desk for advice
Security and protection of data/information	
If you use non corporate issued equipment or use your own equipment to access the organisations email system make sure virus protection is switched on and up to date	Do not use or violate 'copyright' protected information or material (including media, software and information)
If you think you have been attacked or the source of any potential virus or malware notify the IT Service Desk immediately	Do not click on any unknown/unrecognised/unsolicited emails OR attachments
Use the organisations secure email system (CJSM) for the sending of personal/sensitive information. Secure email account can be requested via the on-line IT Service Catalogue	Do not send sensitive information through unsecure email accounts – always use the organisations secure email system (CJSM)
ALWAYS check that you are using correct email addresses (check for correct name and email address)	
Protecting the Organisations Reputation	
	Do not use the organisations email system for sending/stating personal views, comments or opinions
	Do not use the organisations email system for or posting discriminatory, harassing, or threatening messages or images

4.3. Guest Wi-Fi

General guidance	
	Guest Wi-Fi is provided for staff and bonafide visitors/guests to Plumer House to access the Internet, Social Media and other related web activities and web services
	Staff using the guest W-Fi facility must do so in non-working time
	The use of Guest WiFi is less restricted than the corporate PCH internet access. The use and access to internet content via this service (and the consequences) is at the risk of the individual
Do	**Do Not**
Guest Wi-Fi Usage	
Use the guest Wi-Fi to connect various personal devices (e.g. Tablets, Smart Phones)	Do not access or use Guest Wi-Fi services during working time
If you use your own equipment to access the internet, for your protection and safety make sure virus protection is switched on and up to date	Do not click on/open links that are unprompted and/or unexpected and not related to your task. This could lead to ransomware and malware infections!
	Do not use the internet for sending or posting discriminatory, harassing, or threatening messages or images
	Do not use Guest Wi-Fi for sending/stating personal views, comments or opinions

4.4. Social Media

General guidance	
	PCH uses various Social Media sources (Facebook, Twitter, Yammer etc) to engage and communicate with its residents and staff
	PCH also recognises that social is embedded in many people's daily lives. As such, it allows employees to use the internet and to access social media sources for personal reasons provided that it is used outside working time (e.g. outside working/core hours, lunch breaks)
Do	**Do Not**
Social Media Usage	
Only use social media for business purposes if your job role requires it and social media usage has been approved by PCH Management	Do not use personal social media accounts for business purposes
Security and protection of data/information	
	Do not use or violate 'copyright' protected information or material (including media, software and information)
	Do not divulge or share your social media passwords with anyone
Protecting the Organisations Reputation	
	Do not use personal social media accounts for sending or posting discriminatory, harassing, or threatening messages or images
	Do not use personal social media accounts for posting/stating personal views, comments or opinions on business matters

5. Remote working (including using your own equipment)

The ability to work and access IT services/information from remote & external locations is key to enable staff mobility and flexible working to meet business needs.

General guidance	
	PCH recognises that staff need to be able to work flexibly and to be able to work away from their normal place of work. Various IT solutions are available (hardware and services) that enable staff to access applications and information when it is needed.
	PCH IT also allows the access to PC applications and information from non corporate equipment (e.g. home computers).

Do	Do Not
Remote working	
Ensure that any portable equipment issued for remote working is kept safe and protected from damage	One method of remote working is via a 'Vasco' Security token. If you have been issued with a 'Vasco' token, it must not be shared with any other member of staff
Security and protection of data/information	
If you use non corporate issued equipment or use your own equipment for remote working or access to the organisations email system or IT network make sure virus protection is switched on and up to date	Do not attempt to access information to which you do not have any permissions to access
If you think you have been attacked or the source of any potential virus or malware notify the IT Service Desk immediately	Do not divulge or share your PCH IT credentials (user name/password) to anyone
Protecting the Organisations Reputation	
Immediately notify the IT Service Desk if any portable equipment is lost or stolen or broken	Do not use PCH IT systems or services for sending or posting discriminatory, harassing, or threatening messages or images
	Do not use PCH IT systems or services or personal social media accounts for posting/stating personal views, comments or opinions on business matters

6. Information Security

PCH has to comply with various legislation and compliance standards regarding the access, use, storage and retention of personal data. As a major housing provider we hold and manger significant amounts of resident and personal information.

In additional to the usage guidance below it is important that you have read and familiarised yourself with other policies and procedures relation to information security i.e. PCH Data Protection Policy, Information Security Policy. These can be found in the 'Strategies and Policies site' on the PCH Intranet.

General guidance	
	Information is a major business asset that Plymouth Community Homes has a duty and responsibility to protect. This is especially important in the increasingly interconnected business environment, as the Association is now exposed to a growing number and variety of threats and vulnerabilities.

Security and protection of data/information	
Only access information for which you are entitled to or have permission to access	Do not attempt to access information to which you do not have any permissions to access
Adhere to the PCH 'Data Protection Act' obligations	Do not divulge or share your PCH IT credentials (user name/password) to anyone
Change your PCH IT Passwords when prompted to	Never leave your computer screen unlocked and unattended
Notify IT Service Desk immediately if you feel data or information has been compromised (e.g. virus/malware attack, suspect you password has been misused, or anything else that puts the security of our IT systems and data at risk	Do not leave any unattended sensitive printed information (either at the printer or at your workstation)
Ensure that all information (files & documents) are saved/stored in an appropriate area – i.e. suitable area on the SharePoint or Network drives. If in doubt seek advice from your manager, IT Service Desk or the Governance team	Do not click on any unsolicited web page links or open an unsolicited or unexpected email attachments from untrusted sources
	Do not save or transfer corporate / organisation data (files, documents) to untrusted sources (i.e. personal email account, home computer, 3rd party computer)
	Do not save or store any personal or sensitive information in openly available storage areas. If in doubt seek advice from your manager, IT Service Desk or the Governance team

7. Loss & Damage of IT Equipment

General guidance	
	It is your responsibility to look after equipment/hardware (and accessories) issued to you and to use it for the purpose for which is has been issued. This includes the physical well-being/state of equipment and ensuring it is keep safe and secure at all times.

Do	Do Not
Security and protection of data/information	
Report any loss of damage of equipment to IT Service Desk immediately	Do not use equipment in circumstances where damage or loss is likely to occur – i.e. exposure to water or extreme heat
Use equipment/hardware as advised by manufacturer instructions/user guide	Do not leave equipment/hardware (especially portable/mobile equipment) unattended
Return any unused or any wanted equipment/hardware to the IT Service Desk	Do not pass on or reassign any hardware/equipment issued to you to any other work colleague (this must be arranged/co-ordinated by IT Service Desk)

8. Health & Safety

Every employee has a responsibility to protect themselves and work colleagues from risk of injury, hazards or dangerous situations.

It is important that IT equipment is used correctly and does not present any risk or dangers to the employee of fellow colleagues.

General guidance	
	IT equipment involves the use of electrically/battery powered devices and more often than not involves the use of multiple cables and the connection of peripheral equipment (mice, keyboard etc). IT equipment must only be for the purposed for which it is intended and in line with supplier/manufacturer guidelines.

Do	Do Not
Security and protection of data/information	
If you spot or become aware of any hazards or dangerous situations involving the use of IT equipment contact the IT service Desk IMMEDIATELY (i.e. trailing leads, exposed electrical contacts, broken or damaged equipment)	Do not remove any covers or expose the inner working of ant IT equipment
Report any breakages and failure of IT equipment to the IT Service Desk	Do not move or connect cables that may cause a trip hazard or impede movement of staff or obstruct doors, passage ways of access routes for staff
Any non PCH issued IT equipment (i.e. your own devices) that connect to the electrical supply must be PAT tested (contact Facilities team to arrange any PAT testing of electrical equipment)	Do not use or subject IT equipment to conditions that may cause a danger or hazard (i.e. exposure to rain/water)
Do check that you are correctly positioned (posture) to use your IT equipment. Further information and guidance on Posture can be found here	Do not drink or have any liquids placed close to any computer equipment
Take regular breaks especially when using computer monitors for any length of time. Further information and guidance on Posture can be found here	Make sure powered IT equipment is correctly powered / connected and that any power sockets are not overloaded. If in doubt contact the IT Service Desk
Avoid screen glare from surrounding light sources (sun light, lamps etc). Re-position monitor to avoid any screen glare as appropriate	

Further information regarding property and safety can be found on the Property & Safety SharePoint Department Site.

9. Disposal of IT equipment

It is vitally important that PCH acts responsibly in disposing of and recycling of any redundant, surplus or 'beyond repair IT equipment'. PCH also needs to adhere to The Waste Electrical and Electronic Equipment Directive (WEEE).

Not only do we need to ensure we dispose of equipment in a safe and environmentally friendly way but we also need to ensure that any data/information (files, documents etc) are permanently destroyed so to prevent any data breaches/leaks of sensitive, personal and/or commercially sensitive information.

General guidance	
Please be mindful that when requesting the removal or disposal of IT equipment that consideration is given to any information that may be saved/stored on the device (memory cards, hard disks etc) as all information will be permanently wiped from the equipment prior to disposal.	
If you become aware of any old/redundant IT equipment or wish to hand back any IT equipment contact the IT Service Desk who will arrange collection and if required arrange for secure disposal.	
Do	**Do Not**
Security and protection of data/information	
Contact the IT Service Desk if you identify and surplus or redundant IT equipment	Never attempt to dispose of or old/redundant IT equipment. Contact the IT Service Desk who will make the necessary arrangements to collect/remove
Do be mindful of any data (files and documents) that may be stored on any IT equipment that is either redundant or surplus to requirements	Never re-assign any IT equipment to other staff or departments within PCH. This must be arranged via the IT Service Desk so that company asset information can be maintained and kept up to date
	Never offer redundant or surplus equipment to anyone or any organisation outside of PCH