



Doc. Ref:	D&IT - AUP
Issue:	v4
Last reviewed:	October 2024
Next Review date:	October 2025



# **Acceptable Usage Policy**

## **Digital & 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	2
2. Use of Digital & IT within PCH	2
3. Use of Digital & IT Equipment	2
3.1. Digital & IT Usage	3
3.2. Use of Mobile Devices (Phones, Tablets)	4
3.2.1. Corporate Mobile Devices	4
3.2.2. Bring / Use Your Own Device (BYOD/UYOD)	5
4. Use of Internet based services	6
4.1 Internet	6
4.2 Email	7
4.3 Guest WiFi	7
4.4 Social Media	8
5. Remote working (including using your own equipment)	8
6. Information Security	9
7. Access and use of Artificial Intelligence (AI/ChatGPT)	10
8. Loss & Damage of IT Equipment	11
9. Health & Safety	11
10. Disposal of IT equipment	12

## 1. Introduction

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

It is important that any use of Digital IT equipment and services is used in an appropriate way allowing for the flexibility and needs of the organisation and staff whilst meeting its obligations to data security, protection of information and duty of care to company assets (Digital & IT Equipment).

This policy document outlines 'acceptable usage' for various aspects of Digital IT equipment and services and is in addition to '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.

When signing on to your laptop/mobile device you are agreeing to the conditions set out within this 'Acceptable Usage Policy'.

Any abuse or non authorised use of Digital IT equipment, and the services/data it accesses, may be subject to disciplinary action.

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

## 2. Use of Digital & IT within PCH

PCH adopts a flexible approach to the use of various technologies, services and equipment. 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) and the care and protection of technology devices (Laptops, Smartphones, Tablets).

PCH Digital & 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' policy outlined in this document.

## 3. Use of Digital & IT Equipment


PCH makes available various types of equipment to enable staff to fulfil their duties. This section covers 'acceptable usage policy' for core Digital & IT equipment and the services that can be accessed/used.

### 3.1. Digital & IT Usage


A number of general rules, guidelines and recommendations apply to the use of Digital & IT within PCH.

Most of these are common sense and practical measures aimed at allowing staff to do their job whilst being mindful of security, protection of data and care of Digital & IT equipment.


#### System & Network Security

	Do	Do not
	<ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Change your password immediately if you suspect that it may have been compromised or become known by any other person</li> <li><input checked="" type="checkbox"/> Inform the Digital &amp; IT Service Desk immediately if anyone asks you to reveal your password or if you have inadvertently shared personal or sensitive information</li> <li><input checked="" type="checkbox"/> Change your password regularly (as prompted) and avoid using obvious or standard passwords</li> </ul>	<ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> 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 the Digital &amp; IT Service Desk)</li> <li><input checked="" type="checkbox"/> Never share or divulge your password with anyone</li> <li><input checked="" type="checkbox"/> Never attempt to access systems, applications or files to which you are not authorised to do so</li> </ul>

#### Protection from Viruses and Malware (Cyber threats)

	Do	Do not
	<ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Always report any potential 'infections' or attacks or suspicious emails to the Digital &amp; IT Service Desk IMMEDIATELY</li> <li><input checked="" type="checkbox"/> Always use up to date virus checking software to ensure no infections are present on any emails, websites and/or other sources received from outside PCH <b>(all PCH issued devices are issued with installed anti-virus protection software which is automatically updated at regular intervals)</b></li> </ul>	<ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Do not open any untrusted or unexpected emails, attachments or web links – if in doubt contact the Digital &amp; IT Service Desk for advice</li> <li><input checked="" type="checkbox"/> Do not download/install software without prior consent/approval from the Digital &amp; IT Service Desk</li> <li><input checked="" type="checkbox"/> Do not circumvent any existing protection – switching off virus protection or bypassing PCH firewall (security gate)</li> </ul>

#### Protecting the Organisations Reputation

	Do	Do not
	<ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Use PCH standard format for email signature and 'out of office' messages</li> <li><input checked="" type="checkbox"/> Be aware that PCH staff web and email usage is actively monitored (inappropriate use will be dealt with via PCH disciplinary policy)</li> </ul>	<ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Do not express personal views or represent the organisation without management approval</li> <li>Further information/guidance on this is available via the 'Social Media Guidance for PCH Employees' accessible via the Strategies &amp; Policies SharePoint Site</li> <li><input checked="" type="checkbox"/> Do not use or violate 'copyright' protected information or material (including media, software and information)</li> <li><input checked="" type="checkbox"/> Do not access, view or distribute objectionable or biased material or information (i.e. pornographic, racist, terrorism)</li> <li><input checked="" type="checkbox"/> Do not use systems or send emails that discriminate on the basis of race, sex or other biases</li> </ul>

#### Hints & Tips



Avoid, wherever possible, using excessive system resources during peak working hours. An example would be transferring large files between 9 am and 5 pm. Please contact the Digital & IT Service Desk for further guidance



When sharing information (particularly via email) use 'links' to data/documents and avoid sending attachments wherever possible, especially when sending to multiple email addresses. Also consider the use of MS Teams for sharing and collaboration of information, data and files (internally and externally)



Avoid any unnecessary 'CC' or 'BCC' in emails. This causes duplication and unnecessary work



Do not use PCH time or Digital & IT equipment for personal use or business matters not related to PCH unless agreed with your manager and then only in a trustworthy way. Digital & IT systems are monitored and abuse will be dealt with on an individual basis under existing PCH disciplinary procedures

**If in doubt or if you have any concerns or queries please contact the Digital & IT Service Desk**


## 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 as long as you adhere to the appropriate sections of 'Acceptable Usage Policy'.


Mobile devices are defined as a device capable of receiving mobile calls and/or able to access and display corporate information (documents, data and applications). This typically includes mobile phones, phablets, tablets and sim/4G enabled laptops/notebooks.

### 3.2.1. Corporate Mobile Devices


#### Mobile Device Usage

	Do	Do not
	<ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Contact the Digital &amp; IT Service Desk in the event of any equipment failure or breakages</li> <li><input checked="" type="checkbox"/> Do use your mobile devices for taking photographic evidence provided it is in line with your work AND that permission is sought if photo content involves a 3<sup>rd</sup> party (e.g. another person or personal property)</li> <li><input checked="" type="checkbox"/> If prompted to upgrade phone/tablet apps do so when connected to WiFi (e.g. Plumer Guest WiFi/home broadband) to avoid any unnecessary mobile data usage/charges</li> </ul>	<ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> 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</li> <li><input checked="" type="checkbox"/> Do not download or install applications (from Apple, Google and vendor apps store) and/or breach copyright of licensing infringements. If in doubt contact the Digital &amp; IT Service Desk</li> <li><input checked="" type="checkbox"/> 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. Mobile device features such as GPS or Maps, SMS (texting) should only be used for PCH business purposes – i.e. receiving repair notifications via Total Repairs System and only then used when vehicle is stationary and/or safe to do so</li> </ul>

#### Security and protection of data/information

	Do	Do not
	<ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Be aware that PCH mobile phone call/data usage is actively monitored (inappropriate use will be dealt with via the PCH disciplinary policy)</li> <li><input checked="" type="checkbox"/> Be aware that PCH web and email usage is actively monitored (inappropriate use will be dealt with via the PCH disciplinary policy)</li> </ul>	<ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Do not divulge or share your mobile device PIN code with anyone (4 or 6 digit PIN codes are enforced for all corporate mobile devices)</li> <li><input checked="" type="checkbox"/> Do not leave any PCH issued equipment left unattended (this applies in and out of the office)</li> <li><input checked="" type="checkbox"/> Do not leave mobile devices in an unattended vehicle. This includes cars/vans parked in any car park, place of work, in your garage or on your driveway. Mobile devices must not be left in the boot or glove box of your vehicle under any circumstances</li> <li><input checked="" type="checkbox"/> When using mobile devices do not express personal views or represent the organisation without management approval Further information/guidance on this is available via the 'Social Media Guidance for PCH Employees accessible via the Strategies &amp; Policies SharePoint Site</li> <li><input checked="" type="checkbox"/> Do not use or violate 'copyright' protected information or material (including media, software and information)</li> <li><input checked="" type="checkbox"/> Do not access, view or distribute objectionable material or information (i.e. pornographic, racist, terrorism)</li> </ul>

#### Loss / safe keeping of equipment

	Do	Do not
	<ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Immediately notify the Digital &amp; IT Service Desk if equipment is lost, damaged or stolen so that the mobile device can be locked, blocked and/or wiped. 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</li> </ul>	<ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Do not subject or expose your mobile device to situations or adverse conditions that may cause or result in damage (i.e. water, heat)</li> </ul>

## 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 the employment of PCH. Failure to return D&IT equipment will incur costs to the organisation which may involve recovering the costs from the employee and/or costs being crossed charge to departments.

## 3.2.2. Bring / Use Your Own Device (BYOD/UYOD)

### Mobile Device Usage

	Do	Do not
	<ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Do use your mobile devices for taking photographic evidence provided it is in line with your work AND that permission is sought if photo content involves a 3<sup>rd</sup> party (e.g. another person or personal property)</li> <li><input checked="" type="checkbox"/> Ensure you adhere to the appropriate sections of 'Acceptable Usage Policy' when using personal or non PCH issued devices</li> </ul>	<ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> No reimbursement for business calls made on personally owned mobile devices will be made to employees other than in exceptional circumstances and agreed by PCH Management</li> <li><input checked="" type="checkbox"/> No reimbursement for any use or breach of personal tariff (voice or data) due to corporate use of personal device</li> </ul>

### Security and protection of data/information

	Do	Do not
	<ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> 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 Intune Mobile Device Management software unless agreed by PCH Management and must use current and supported Operating System (OS) and applications (apps)</li> </ul>	<ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Do not divulge or share your mobile device PIN code with anyone</li> <li><input checked="" type="checkbox"/> Do not download, save or store any PCH/corporate information or files on your personal or non issued PCH device</li> <li><input checked="" type="checkbox"/> Do not attempt to uninstall PCH device control software (MFA, MS Intune/corporate apps store). If you no longer wish to use your own device for business purposes please contact the Digital &amp; IT Service Desk</li> </ul>

### Loss / safe keeping of equipment

	Do	Do not
	<ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Immediately notify the Digital &amp; IT Service Desk if your personal equipment is lost or stolen (if it has been used for business purposes)</li> </ul> <p>PCH Digital &amp; IT will be able to lock and remotely delete any corporate data or apps held on your personal device using remotely control mobile device management software</p>	<ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> PCH is not responsible and will not reimburse any loss arising from the use of personal devices for corporate purposes (e.g. lost, stolen or damaged)</li> </ul>

## General Guidance



PCH welcomes enquiries from staff to use their own mobile device. PCH Digital & IT have arrangements in place that enables staff to use their mobile phones 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 your normal working hours. Any work carried out will, unless otherwise agreed with management, be your choice and unpaid.

## 4. Use of Internet based services


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

However, we need to be mindful that Internet 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 of the internet, email, social media, Plumer guest and public Wi-Fi facilities.

### 4.1 Internet


#### Internet Usage

	Do	Do not
	<p><input checked="" type="checkbox"/> Use the intranet to access work related information, research and tasks</p>	<p><input checked="" type="checkbox"/> Do not use / access internet during working time for non work related tasks, actions or information. Any abuse of the internet may result in disciplinary actions under the PCH disciplinary policy</p>








#### Security and protection of data/information

	Do	Do not
	<p><input checked="" type="checkbox"/> 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</p> <p><input checked="" type="checkbox"/> If you think you have been compromised, attacked or the source of any potential virus or malware notify the Digital &amp; IT Service Desk immediately</p>	<p><input checked="" type="checkbox"/> Do not use or violate 'copyright' protected information or material (including media, software and information)</p> <p><input checked="" type="checkbox"/> 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!</p>

#### Protecting the Organisation's Reputation

	Do	Do not
	<p><input checked="" type="checkbox"/> Do ensure that all communications and content shared online are professional, respectful, and in line with PCH's values and ethics to maintain the company's reputation</p>	<p><input checked="" type="checkbox"/> Do not use the internet for sending or posting discriminatory, harassing, or threatening messages or images. Any use of the internet (including social media) must adhere to PCH Social Media Guidance which can be accessed via the Strategies &amp; Policies SharePoint Site</p> <p><input checked="" type="checkbox"/> Do not use the internet for sending/stating personal views, comments or opinions</p> <p>Further information/guidance on this is available via the 'Social Media Guidance for PCH Employees accessible via the Strategies &amp; Policies SharePoint Site</p>

#### 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, within lunch breaks)
-  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.
-  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 Digital & IT Service Desk
-  Certain internet sites and content are filtered and/or restricted to protect the organisation and staff from risks and unsuitable information/pictures (content)

## 4.2 Email

### Email Usage, Protection and Security

	Do	Do not
	<ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Use the organisation Email system only for business related matters</li> <li><input checked="" type="checkbox"/> If you use non corporate issued equipment or use your own equipment to access the organisations email system make sure anti-virus protection is switched on and up to date and PIN protected (or suitable lock screen protection)</li> <li><input checked="" type="checkbox"/> If you think you have been compromised, attacked or have been subject to any potential virus or malware notify the Digital &amp; IT Service Desk IMMEDIATELY</li> <li><input checked="" type="checkbox"/> Use the organisations secure email system (CJSM) for the sending of personal/sensitive information. Secure email accounts can be requested via the Digital &amp; IT Service Desk or via the on-line Digital &amp; IT Service Catalogue</li> <li><input checked="" type="checkbox"/> Always check email addresses that you are sending email to so that you do not send emails to unintended recipients</li> </ul>	<ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> <b>Do not:</b> <ul style="list-style-type: none"> <li>• Open any emails that are unsolicited, unexpected or from an unknown source without making checks first to check it is a valid/bona fide email. If in doubt, ask Digital &amp; IT Service Desk to check for you</li> <li>• Click on any links with emails to download or install any software. If you have a requirement contact the Digital &amp; IT Service Desk for advice</li> <li>• Never disclose personal or sensitive information to an unknown source</li> </ul> </li> <li><input checked="" type="checkbox"/> Do not use or violate 'copyright' protected information or material (including media, software and information)</li> <li><input checked="" type="checkbox"/> Do not send sensitive information through unsecure email accounts – always use the organisations secure email system (CJSM)</li> <li><input checked="" type="checkbox"/> Do not use the organisations email system for sending/stating personal views, comments or opinions</li> <li><input checked="" type="checkbox"/> Do not use the organisations email system to send or post discriminatory, harassing, or threatening messages or images (content)</li> </ul>

### 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

## 4.3 Guest WiFi

	Do	Do not
	<ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Use the guest Wi-Fi to connect various corporate and personal devices (e.g. Laptops, Tablets &amp; Smart Phones)</li> <li><input checked="" type="checkbox"/> If you use your own equipment to access the internet, for your protection and safety make sure anti-virus protection is switched on and up to date</li> </ul>	<ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Do not access or use Guest Wi-Fi services during working time for non working activities</li> <li><input checked="" type="checkbox"/> Do not click on/open links that are unprompted and/or unexpected and not related to your work or tasks. This could lead to the risk of ransomware and malware infections!</li> <li><input checked="" type="checkbox"/> Do not divulge or share your device and/or social media passwords with anyone</li> <li><input checked="" type="checkbox"/> Do not use personal social media accounts for sending or posting discriminatory, harassing, or threatening messages or images</li> <li><input checked="" type="checkbox"/> Do not use personal social media accounts for posting/stating personal views, comments or opinions on business matters</li> </ul> <p>Further information/guidance on this is available via the 'Social Media Guidance for PCH Employees accessible via the Strategies &amp; Policies SharePoint Site</p>

### General Guidance



Guest Wi-Fi is provided for staff and bona fide 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



## 4.4 Social Media

	Do	Do not
	<ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Only use social media for business purposes if your job role requires it and social media usage has been approved by PCH Management</li> </ul>	<ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Do not use personal social media accounts for business purposes</li> <li><input checked="" type="checkbox"/> Do not use or violate 'copyright' protected information or material (including media, software and information)</li> <li><input checked="" type="checkbox"/> Do not divulge or share your social media passwords with anyone</li> <li><input checked="" type="checkbox"/> Do not use personal social media accounts for sending or posting discriminatory, harassing, or threatening messages or images</li> <li><input checked="" type="checkbox"/> Do not use personal social media accounts for posting/stating personal views, comments or opinions on business matters</li> </ul> <p>Further information/guidance on this is available via the 'Social Media Guidance for PCH Employees accessible via the Strategies &amp; Policies SharePoint Site</p>

### 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 media 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)

## 5. Remote working (including using your own equipment)

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

	Do	Do not
	<ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Ensure that any portable equipment issued for remote working is kept safe and protected from damage</li> <li><input checked="" type="checkbox"/> 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 anti-virus protection is switched on and up to date and must use current and supported Operating System (OS) and applications (apps)</li> <li><input checked="" type="checkbox"/> If you think you have been compromised, attacked or the source of any potential virus or malware notify the Digital &amp; IT Service Desk immediately</li> </ul>	<ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Do not attempt to access information to which you do not have any permissions to access</li> <li><input checked="" type="checkbox"/> Do not divulge or share your PCH IT credentials (user name/password) with anyone</li> <li><input checked="" type="checkbox"/> Do not use PCH Digital &amp; IT systems or services for sending or posting discriminatory, harassing, or threatening messages or images</li> <li><input checked="" type="checkbox"/> Do not use PCH Digital &amp; IT systems or services or personal social media accounts for posting/stating personal views, comments or opinions on business matters</li> </ul> <p>Further information/guidance on this is available via the 'Social Media Guidance for PCH Employees accessible via the Strategies &amp; Policies SharePoint Site</p>

### 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 Digital & IT also allows the access to applications and information from non corporate equipment (e.g. home computers) provided that usage of personal devices adheres to the appropriate policies within this 'Acceptable Usage Policy'.

## 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 manage 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.*

	Do	Do not
	<input checked="" type="checkbox"/> Only access information for which you are entitled to or have permission to access	<input checked="" type="checkbox"/> Do not attempt to access information to which you do not have any permissions to access
	<input checked="" type="checkbox"/> Adhere to the PCH 'Data Protection Act' obligations	<input checked="" type="checkbox"/> Do not divulge or share your PCH IT credentials (user name/password) with anyone
	<input checked="" type="checkbox"/> Change your PCH IT Passwords when prompted to	<input checked="" type="checkbox"/> Never leave your computer screen unlocked and unattended
	<input checked="" type="checkbox"/> Notify Digital & IT Service Desk immediately if you feel data or information has been compromised e.g. virus/malware attack, suspect your password has been misused, or anything else that puts the security of our Digital & IT systems and data at risk	<input checked="" type="checkbox"/> Do not leave any unattended sensitive printed information (either at the printer or at your workstation) <input checked="" type="checkbox"/> Do not click on any unsolicited web page links or open any unsolicited or unexpected email attachments from untrusted sources
	<input checked="" type="checkbox"/> Ensure that all information (files & documents) are saved/stored in an appropriate area – i.e. suitable area on SharePoint, Teams, OneDrive or Network drives. If in doubt seek advice from your manager, Digital & IT Service Desk or the Governance team	<input checked="" type="checkbox"/> Do not upload any corporate information or data to cloud based services unless they are PCH approved/authorised cloud applications or services

### 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.

**DATA**  
PROTECTION

## 7. Access and use of Artificial Intelligence (AI/ChatGPT)

Artificial Intelligence (AI) is fast emerging in many aspects of the digital and technological world and is never far from the news! AI has now evolved to the point where it can be accessed and used by almost anyone. ChatGPT has led the AI revolution from an 'end user' perspective. The use of AI via ChatGPT (and other AI applications such as Bing, MS Co-Pilot, Google Gemini, Apple Intelligence) can be useful, beneficial and helpful. HOWEVER, AI accesses and uses many sources of data and information across the internet and filters/presents this information based on algorithms and machine learning (often referred to as LLML). As a result, there are many risks including information accuracy, bias, confidentiality, copyright infringement and ethical use. It is important that you are aware of the limitations and risks in the use of any AI system.

### General Guidance



#### Accuracy

All information generated by AI must be reviewed and edited for accuracy prior to use. You are responsible for reviewing all AI output, and are accountable for ensuring the accuracy of AI generated output before use/release. **If you have any doubt about the accuracy of information generated by AI, it should NOT be used.**



#### Confidentiality/Business/Personal Information

Confidential, business or personal information must not be entered into any AI tool, as any information entered will be subsequently made available in the public domain. **If you have any doubt about the confidentiality of information, you should not use AI.**



#### Ethical Use

AI must be used ethically and in compliance with all applicable legislation, regulations and PCH policies. You must not use AI to generate content that is discriminatory, offensive, or inappropriate.



#### Copyright

You must adhere to copyright laws when utilising AI. It is prohibited to use AI to generate content that infringes upon the intellectual property rights of others, including but not limited to copyrighted material.




#### Legal compliance

Data entered into AI may enter the public domain. This can release corporate, confidential and sensitive information into the public domain and breach regulatory requirements, customer or vendor contracts, or compromise intellectual property. Any release of private/personal information without the authorisation of the information's owner could result in a breach of relevant data protection laws.




#### Bias and discrimination

AI may make use of and generate biased, discriminatory or offensive content. **You should use AI responsibly and ethically and in compliance with PCH policies and applicable laws and regulations.**

	Do	Do not
	<ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> DO double check and sanitise information generated by AI for accuracy</li> <li><input checked="" type="checkbox"/> DO double check and sanitise information generated by AI for bias, discrimination and/or offensive content</li> <li><input checked="" type="checkbox"/> DO check any copyright infringement. AI sources and uses information pulled from shared by others and may be subject to copyright</li> </ul>	<ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> DO NOT share personal, corporate or sensitive information with AI apps or AI enabled web browsers. All information shared with AI will become available in the public domain and used by other AI users</li> <li><input checked="" type="checkbox"/> DO NOT use any AI generated information if you are unsure of its accuracy</li> <li><input checked="" type="checkbox"/> DO NOT use AI generated information if you are unsure on any of the point listed under 'General Guidance' section above.</li> </ul>

## 8. Loss & Damage of IT Equipment

	Do	Do not
	<ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Report any loss or damage of equipment to the Digital IT Service Desk immediately</li> <li><input checked="" type="checkbox"/> Use equipment/hardware as advised by manufacturer instructions/user guide</li> <li><input checked="" type="checkbox"/> Return any unused or any wanted equipment/hardware to the Digital &amp; IT Service Desk</li> </ul>	<ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Do not use equipment in circumstances where damage or loss is likely to occur – i.e. exposure to water or extreme heat</li> <li><input checked="" type="checkbox"/> Do not leave equipment/hardware (especially portable/mobile equipment) unattended</li> <li><input checked="" type="checkbox"/> Do not pass on or reassign any hardware/equipment issued to you to any other work colleague (this must be arranged/co-ordinated by Digital &amp; IT Service Desk)</li> </ul>

### 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 it has been issued. This includes the physical well-being/state of equipment and ensuring it is kept safe and secure at all times.

## 9. 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 Digital & IT equipment is used correctly and does not present any risk or dangers to the employee or fellow colleagues.

	Do	Do not
	<ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> If you spot or become aware of any hazards or dangerous situations involving the use of Digital &amp; IT equipment contact the Digital &amp; IT service Desk IMMEDIATELY</li> <li><input checked="" type="checkbox"/> Report any loss, breakages and failure of Digital &amp; IT equipment to the Digital &amp; IT Service Desk</li> <li><input checked="" type="checkbox"/> Any non PCH issued IT equipment (i.e. your own devices) that connects to PCH electrical supply must be PAT tested (contact Facilities team to arrange any PAT testing of electrical equipment)</li> <li><input checked="" type="checkbox"/> Do check that you are correctly positioned (posture) to use your Digital &amp; IT equipment.</li> <li><input checked="" type="checkbox"/> Take regular breaks especially when using computer monitors for any length of time.</li> <li><input checked="" type="checkbox"/> Avoid screen glare from surrounding light sources (sun light, lamps etc). Re-position monitor to avoid any screen glare as appropriate</li> </ul>	<ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Do not remove any covers or expose the inner working of any Digital &amp; IT equipment</li> <li><input checked="" type="checkbox"/> Do not move or connect cables that may cause a trip hazard or impede movement of staff or obstruct doors, passageways, or access routes for staff</li> <li><input checked="" type="checkbox"/> Do not use or subject Digital &amp; IT equipment to conditions that may cause a danger or hazard (i.e. exposure to rain/water)</li> <li><input checked="" type="checkbox"/> Do not drink or have any liquids placed close to any computer equipment</li> <li><input checked="" type="checkbox"/> Make sure Digital &amp; IT equipment is correctly powered / connected and that any power sockets are not overloaded. If in doubt contact the Digital &amp; IT Service Desk</li> </ul>

### General Guidance



Digital & 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).

Digital & IT equipment must only be for the purpose for which it is intended and in line with supplier/manufacturer guidelines.

## 10. 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.



Do	Do not
<ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Contact the Digital &amp; IT Service Desk if you identify and surplus or redundant Digital &amp; IT equipment</li> <li><input checked="" type="checkbox"/> Do be mindful of any data (files and documents) that may be stored on any Digital IT equipment that is either redundant or surplus to requirements</li> </ul>	<ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Never attempt to dispose of old/redundant Digital &amp; IT equipment. Contact the Digital &amp; IT Service Desk who will make the necessary arrangements to collect/remove any surplus equipment</li> <li><input checked="" type="checkbox"/> Never re-assign any Digital &amp; IT equipment to other staff or departments within PCH. This must be arranged via the Digital &amp; IT Service Desk so that company asset information can be maintained and kept up to date</li> <li><input checked="" type="checkbox"/> Never offer redundant or surplus equipment to anyone or any organisation outside of PCH</li> </ul>

### General Guidance



Please be mindful that when requesting the removal or disposal of Digital & 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 Digital & IT equipment or wish to hand back any Digital & IT equipment contact the Digital & IT Service Desk who will arrange collection and if required arrange for secure disposal.