IT ACCEPTABLE USE POLICY

Change Control

Version	2
Date Approved by CEO	19/08/21
Date Approved by Board	
Post of Policy Holder	CEO Sally Garratt
Date Issued	September 21
Review Date	September 22

IT ACCEPTABLE USE POLICY

CONTENTS

IT ACCEPTABLE USE POLICY

1. PURPOSE

1.1 The Petty Pool College offers a wide range of IT Resources which are free to use for their Users.

1.2 To use the Petty Pool College IT Resources, Users must agree to the responsibilities and conditions outlined in this IT Acceptable Use Policy.

1.3 If you do not agree or understand any aspect of this policy you must logout, disconnect or stop using the IT Resource immediately.

2. SCOPE

2.1 This policy covers:

All companies and subsidiaries of the Petty Pool College

Anyone who uses any Petty Pool College IT resources or services (including Outdoor Centre services)

3. POLICY STATEMENT
User Accounts & Access Control

3.1 Access to The Petty Pool College IT Resources are available via a User Account associated with an individual user.

3.2 Attempting to create, circumvent or elevate permissions of Users Accounts by any other method will result in disciplinary or legal action.

3.3 Users must take all necessary precautions to prevent unauthorised access to their user accounts. This includes ensuring they do not share, loan, write down, email, publish or communicate their User Account details.

3.4 Attempting to obtain another User Account's details by any method will result in disciplinary or legal action.

3.5 Staff maybe required to assist Learners with User Account details this must only be done with the Learners consent each time it is required.

User Account Creation

3.6 Staff Accounts

- HR Manager will request User Accounts for staff via the New User Request Form.

3.7 Learner Accounts will be created 24 hours after being enrolled on an active course

IT ACCEPTABLE USE POLICY

User Account Removal

3.8 Staff Accounts

- Staff User Accounts will be automatically deactivated on the end date of their contract.

3.9 Learners Accounts

- Learners' User Accounts can be disabled at any time by a member of SMT contacting the IT Helpdesk. All non-active Learners User Accounts will be automatically disabled on the completion of their course.

Guest / Generic Accounts

3.10 Petty Pool College do not provide Guest / Generic User accounts.

3.11 All user accounts must be associated to an individual, except where approved by the Head of MIS

3.12 Guest WIFI is available for visitors please refer to the BYOD section for more information

Administration Accounts

3.13 Administration permissions to the domain and local computers is limited to members of the MIS Department.

3.14 Special access and administration permission to systems and applications will only be granted with the system owner's permission or with SMT approval.

3.15 The number of User Accounts assigned special access or administration permissions will be typically limited to 5 User Accounts per system.

3.16 Special access & administration group membership will be monitored and reviewed annually.

Access Control

3.17 Access to systems and resources are restricted by permissions. To request additional access please contact the IT Helpdesk for guidance.

3.18 Access to IT Resources may be removed by system owners, the HR department or a member of SMT by contacting the IT Helpdesk (it@pettypool.org.uk).

3.19 All requests for permission changes must be requested by email, an IT helpdesk call will be raised for all permission changes as an audit record.

3.20 The MIS Department regularly monitor file access permissions

IT ACCEPTABLE USE POLICY

Passwords & Authentication

3.21 Petty Pool College requires all User Accounts to have a complex Password, details of the complex password requirements are detailed in Appendix B

- Passwords must not be obvious or easy to guess
- Passwords must be unique and must not be used for any other purpose or website.
- Passwords must be memorised and may not be written or saved on electronic devices.
- Passwords may be changed at any time. Please contact the IT Helpdesk for further assistance or advice on passwords.
- Passwords must remain strictly confidential, should never be written down or disclosed to anyone.
- Users are responsible for any activity which takes place while logged in using their User Account.
- User Accounts will automatically be locked out after 5 incorrect password attempts.

3.22 The National Cyber Security Centre (NCSC) have published an article called “Three random words or #thinkrandom” which provides guidance on what makes a good password

3.23 The NCSC Password Policy Infographic explains how passwords are discovered & how system security policies can help.

Reduce Reliance on passwords

3.24 Petty Pool College aim to use single sign on (SSO) where available to reduce the number of passwords Users are required to remember & enter

Multi Factor Authentication (MFA) or Two Factor Authentication (2FA)

3.25 To improve the security of your user account MFA can be enable by contacting the IT Helpdesk

3.26 User Accounts with access to highly sensitive information including all members of the IT department must have MFA enable.

3.27 MFA can be requested on any User Account via the IT Helpdesk

3.28 The IT Department may require User Accounts to have MFA enable if it is identified that their User Account is being targeted by a cyber-threat.

Password Managers

3.29 A password manager is an app on within your web browser that stores your passwords securely, so you don’t need to remember them all, making it easier to log on. They can also create random, unique passwords for you, when you need to create a new password (or change an existing one).

IT ACCEPTABLE USE POLICY

Data Security

3.30 To ensure the data security, the College has a clear screen & desk policy, this means:

- Computers must be locked EVERY TIME you leave your computer or desk, even if it is only for a short period of time.
- All printed documents with personal information must be kept in a locked draw or cabinet EVERY TIME you leave your desk.
- Passwords must never be shared; if someone else knows your password, please change it immediately. If someone else needs access to documents, emails, systems etc. please contact the IT Helpdesk for advice.

3.31 Documents and data containing personal data must never be taken, copied or downloaded onto personal computers or systems outside of the College's network. Please refer to the Information Security Policy for more details.

Monitoring and Logging

3.32 The Petty Pool College monitor and log data for all IT Resources.

3.33 Monitoring and logging includes:

- Login / Logout
- File Activity
- Internet Activity
- Communication
- Location Tracking of equipment
- Screen capture

3.34 By logging into IT Resources you agree that data identifying you as an individual can be securely stored and used by the Petty Pool College to investigate breaches of this policy.

3.35 Where officially requested, this data will be sent to local authorities for criminal investigations.

Safeguarding and Prevent

3.36 The following activity is actively monitored and logged as part of the Colleges responsibility towards multi- agency safeguarding and PREVENT agendas.

• Information which may lead to potential terrorism or extremist activity o Internet activity including sites categorised as:

- Intolerance
- Personal Weapons
- Terrorism
- Violence

• Information which may lead to a potential risk to young people or vulnerable adults

- Internet activity including sites categorised as:

  - Adult Entertainers
  - Adult Sites
  - Child Abuse
  - Pornography
  - Restricted to Adults

3.37 Logs and information relating to Safeguarding or Prevent will be shared with the College's trained Safeguarding / Prevent officer and may be shared with local authorities for further investigation.

Vandalism

3.38 Acts of vandalism are taken very seriously. Anyone caught vandalising IT Resources will result in disciplinary and/or legal proceedings.

3.39 Any costs incurred repairing or replace vandalised equipment will be charged to anyone caught vandalising IT Resources.

3.40 To minimise the risk of accidental damage to IT equipment, Food & Drink is not permitted in any Library Plus or computer suites.

3.41 Users are not permitted to unplug or move any non-mobile IT Resources.

Software

3.42 Users are not permitted to install software on any IT Resources this includes running portable applications.

3.43 The installation of software applications can be requested via the IT Helpdesk.

3.44 Use of cloud-based software applications which store personal information of learners or staff must be approved by the MIS Manager or SMT

Viruses & Malware

3.45 The Petty Pool College use a number of security systems to protect data and IT Resources from viruses and malware.

3.46 Users must report to the IT Helpdesk if a computer virus has been identified.

3.47 Attempts to circumvent any security systems, including Anti-Virus software will result in disciplinary and/or legal action

3.48 Attempts to execute files, scripts or code known to be malicious will result in disciplinary and/or legal action.

IT ACCEPTABLE USE POLICY

Internet Access

3.49 The Petty Pool College E-Safety & Social Media Policy details acceptable online behaviours and electronic communication and the additional responsibilities which you must accept before accessing Social Media sites.

3.50 The College uses a web filtering solution to block access websites which may contain inappropriate content, non-educational content or present a security concern. Just because content is not filtered out does not mean it is OK to access.

3.51 The College monitors and logs all usage of the Internet.

3.52 Downloading or streaming of copyrighted material which you are not licenced to view / access will result in disciplinary or legal action.

3.53 The use of Peer to Peer software including BitTorrent is not permitted to run while connected to any Petty Pool College networks.

3.54 Access to the Dark Web or Tor Networks is not permitted while connected to any Petty Pool College networks.

3.55 Users must not connect or tether to any IT Resources to any other networks or internet connections without approval from the MIS Manager or SMT.

3.56 Misuse of Petty Pool College Internet Access or any attempt to circumvent security systems including web filtering will result in disciplinary and/or legal action. Should be reported to the IT Helpdesk immediately.

Bring Your Own Device (BYOD)

3.57 **Users** may connect their own devices to the College Guest WIFI service using their **User Account** details. **Users** must agree to the College IT Acceptable Use policy to use this service.

3.58 **Users'** Own Devices may be connected by WIFI only, connecting via Ethernet cable is not permitted.

3.59 The activity of **Users'** Own Devices are monitored and logged. Devices may be blocked if in breach of this policy or considered to be a security risk.

3.60 IT support services are unable to support **Users'** own devices, including the recovery of data. If experiencing issues, please use the **IT Resources** supplied by The Petty Pool College.

3.61 Personal Hotspots or Bring Your Own Network (BYON) is not permitted.

3.62 Use of anonymizing, VPN or proxy software is not permitted on any Petty Pool College networks.

3.63 Own devices are used, connected and configured at the **Users'** own risk.

IT ACCEPTABLE USE POLICY

Remote Working

3.64 While working away from the office, special considerations must be made to your working environment and the people around you to ensure data security.

3.65 Data containing personal or sensitive information must not be taken out on the College unless encrypted.

3.66 Users must assess their environment and position of screens so they cannot be viewed by others.

3.67 IT Resources must not be connected to any unsecure public WIFI networks.

• Further guidance on the use of public WIFI is available from the NCSC website: https://www.ncsc.gov.uk/collection/end-user-device-security?curPage=/collection/end-user-device- security/eud-overview/common-questions#wifi

3.68 Remote access to the College Domain is only available via equipment purchased by the College

3.69 VPN access is not available for personal devices.

3.70 Users are required to provide a mobile phone number or download a mobile app to receive a Multi Factor Authentication (MFA) code to access college systems from outside of the office.

• College mobile phones will not be issued to solely facilitate MFA purposes

Loan Equipment

3.71 IT Resources may be available for Users to take off site.

3.72 A Loan Equipment Form must be signed agreeing to the terms and conditions of the loan before any loaned IT Resources are taken off site.

3.73 All devices must be collected in person, devices will not be issued to anyone else.

3.74 Users sign to confirm they have received the loaned IT Resources and it is signed back in when returned

3.75 Loaned IT Resources must only be used by the user who it has been configured for and who has signed the Loan Equipment Form.

3.76 Loaned IT Resources must not be used by:

- Any member of staff other than who has signed the Loan Equipment Form
- Any learner
- Any friends or family member
- Anyone other than the User who has signed the Loan Equipment Form

3.77 The geographic location of College owned equipment may tracked.

IT ACCEPTABLE USE POLICY

3.78 Users must apply any security updates for loaned IT Resources within 5 working days of being notified an update is available.

3.79 Any loaned IT Resources not updated within 5 working days will be disabled and the loaned IT Resources must be returned to the IT Department with the next 5 working days.

3.80 The IT Department reserve the right to request the return of loaned IT Resources at any time.

3.81 Loaned IT Resources must be returned to the IT Department within 5 working days of a return being requested.

3.82 Loaned IT Resources are vulnerable to theft and must never be left within view of the public including within vehicles. Kensington Locks are available via the IT Helpdesk if required.

3.83 It is recommended that Users check that loaned IT Resources are covered by home and car Insurance policies in the event of theft.

3.84 Users may be invoiced for the repair or replacement of any lost or damaged loaned IT Resources.

3.85 Users may be invoiced for any equipment which has not been returned to the IT Helpdesk within 5 days of it being requested.

3.86 IT Resources must never be used while driving.

3.87 Call, data and message costs are monitored. Users will be changed for excessive personal usage.

3.88 College issued mobile devices are pre-configured with a pin to help protect loss of data from theft.

User are reminded that the pin is only effective if the thief does not have access to or cannot obtain or guess the Pin or Users password.

PIN codes and passwords must be secured at all times and most not be kept with the device.

3.89 If a mobile device has been lost or stolen it must be reported to the IT Helpdesk immediately.

Data Security, Removable Media & Backups

3.90 Personal & Confidential information must never be sent or saved to personal accounts or devices. This includes:

- Personal email accounts
- Personal cloud accounts including accounts you have created yourself with your College email address
- USB drives, recordable media and personal storage devices
- Personal computers, laptops, tablets, phones etc...

3.91 Emails, documents & data may be accessed via the mobile apps and web browsers, but personal & confidential information must never be saved to personal devices. If in doubt, please contact it.helpdesk@pettypool.org.uk for advice.

IT ACCEPTABLE USE POLICY

3.92 Personal & Confidential information may only be shared with external companies, contractors or individuals where a data sharing agreement and/or Non-Disclosure Agreement (NDA) has been signed by both parties.

3.93 Personal & Confidential information must only be sent to permitted external companies, contractors or individuals using a secure encrypted method of transfer. For advice please contact it.helpdesk@pettypool.org.uk

3.94 All data must be saved to approved College servers or services.

3.95 Backups of Personal & Confidential information by Users is not permitted.

3.96 All IT Resources must be configured and connected to a Petty Pool College domain by the MIS / IT Department.

Non-Work-Related Data and Documents

3.97 Only data relating to the Petty Pool Colleges' business are to be saved on College servers, systems or databases.

3.98 Private & Personal non-work-related media, data, documents and records must never be saved to any Petty Pool College servers, systems or databases.

3.99 Petty Pool College are not responsible for maintaining the security, retention or any legal requirements of any private or personal non-work-related data stored on College servers or systems or databases.

3.100 Petty Pool College reserves the rights to delete or prevent access to any private or personal non-work-related stored on College servers or systems or databases at any time and without notice.

3.101 At the end of employment contracts Staff are not permitted to transfer any data from College servers, systems or databases without agreement from the HR department.

IT Resource Requests & Disposal

3.102 Additional IT Resources are generally requested within the annual strategic planning process.

3.103 IT Resources must be purchased in accordance with the Financial Regulations and Procurement Strategy.

3.104 IT resources required in year must be approved by SMT before placing orders

3.105 All IT Resources must be disposed via the MIS / IT Department using a registered IT disposal company with ISO 27001 data security and in accordance with Waste Electrical and Electronic Equipment recycling (WEEE) Directive.

3.106 The sale or donation of any Petty Pool College IT Resources is not permitted.

3.107 Upon request or leaving employment all IT Resources must be returned to the IT Helpdesk.

3.108 If IT Resources need to be reallocated, they must be returned to the IT Helpdesk first for reallocation

IT ACCEPTABLE USE POLICY

IT Support

3.109 All issues/incidents with IT equipment or systems must be reported to the IT Helpdesk.

3.110 All IT issues and requests are logged, prioritised and tracked to resolution.

3.111 To log an IT support call, you will be asked for the computer name, location, login name and a detailed description of the problem.

3.112 All criminal incidents will be reported to Action Fraud for legal investigation.

4 RESPONSIBILITIES

Compliance, Monitoring and Review

4.1 Petty Pool College Governing Body is responsible for: • Approval of this policy

4.2 Petty Pool College Senior Management Team is responsible for:

- Recommending approval of policy to the Trustee body
- Ensure this policy reinforces the strategic objectives of the College

4.3 Head of MIS / IT is responsible for:

- Ensure this policy meets legal & regulatory requirements
- Ensure a robust, risk-based approach to cyber security
- Ensure a flexible approach to IT delivery
- Investigate any breach of policy.
- Report any IT related concerns to Chief Operating Officer

4.4 All Information Users are responsible for:

- Ensuring compliance with this policy
- Understand their personal responsibilities in relation to the use of IT Resources
- Reporting suspected breaches of this policy to the IT Helpdesk for investigation

Reporting

4.5 No additional reporting is required.

Records management

4.6 Staff must maintain all records relevant to administering this policy including the maintenance of the IT Asset Register and IT Security log.

IT ACCEPTABLE USE POLICY

5 DEFINITIONS

Terms and definitions

Information Assets: Any form of information, document or data which has a value to the Petty Pool College

Information Security Incident: An event which has caused or could lead to compromising the Confidentiality, Integrity or Accessibility (CIA) of an Information Asset

Information Security Management System (ISMS): Collection of policies and procedures which define how the College manage information Assets

Information Security Steering Group (ISSG): Collection of policies and procedures which define how the College manage information Assets

Information Security: Protecting against the unauthorized use of Information Assets
Information Users: Any members of staff, learner, associate, partner and stakeholder who interact with Petty Pool College Information Assets

IT Helpdesk – Support desk for IT services contact it.helpdesk@pettypool.org.uk
IT Resources – include Computers, laptops, iMacs, Mac books tablets, mobile phones, desktop phones, equipment, software, services, systems, Access to WIFI, etc.

IT Resources: Includes Computers, laptops, iMacs, Mac books tablets, mobile phones, desktop phones, equipment, software, services, systems, Access to WIFI, etc...

Multi Factor Authentication (MFA): A code sent to a mobile by SMS message or via an App which is required to login as well as your password

User Account : Username & Password used to login to the Petty Pool College network **Users :** Enrolled students, members of staff and associates

6 RELATED LEGISLATION AND DOCUMENTS

Legislation

Users are responsible for complying with all legal requirements while using the Colleges IT Resources including but not limited to:

- The Computer Misuse Act 1990
- The Data Protection Act 2018
- The Obscene Publications Act 1959
- The Copyright, Designs and Patents Act 1988
- The Regulation of Investigatory Powers Act 2000
- The Communications Act 2003
- The Digital Economy Act 2010
- The Malicious Communication Act 1988
- Counter Terrorism and Security Act (2015)

IT ACCEPTABLE USE POLICY

Other Policies & Procedures

- IT Security Policy (PPCIT-50002)
- Data Sharing Agreement (PPC-50003)
- Information Security Policy (PPC-50004)

3rd Party Policies, Procedures, Terms & Conditions

Users are responsible for complying with all agreements / terms and conditions while using IT resources including but not limited to:

- Software / Website Licence Agreements
- Software / Website Terms & Conditions
- Copyright Agreements

IT ACCEPTABLE USE POLICY

9 APPENDIX A

Complex Password Rules

The following rules apply to all **User Account** passwords:

- a minimum of 8 characters long
- must not contain the User's : First, Middle or Last Names
- must not have been used before
- must be changed every 60 days.
- must contain characters from three of the following five categories:
    1. Uppercase characters of European languages (A through Z, with diacritic marks, Greek and Cyrillic characters)
    2. Lowercase characters of European languages (a through z, sharp-s, with diacritic marks, Greek and Cyrillic characters)
    3. Base 10 digits (0 through 9)
    4. Non-alphanumeric characters: ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/
    5. Any Unicode character that is categorized as an alphabetic character but is not uppercase or lowercase.