



# **Prior Pursglove and Stockton Sixth Form College**

## **COMPUTER USERS' CODE OF CONDUCT**

---

July 2023

# PRIOR PURSGLOVE & STOCKTON SIXTH FORM COLLEGE

## Computer Users' Code of Conduct

This Code of Conduct contains rules and guidelines which are designed to prevent avoidable network problems and to ensure that the College's networks are kept secure and efficient. The College reserves the right to revise this Code of Conduct and will post the current document on the College SharePoint site. Users are responsible for reading this Code of Conduct regularly.

**VIOLATION OF THIS CODE WILL LEAD TO THE SUSPENSION OF THE USER'S ACCOUNT AND THE MATTER WILL BE REPORTED TO THE PRINCIPAL WHO WILL DETERMINE THE DISCIPLINARY ACTION WHICH SHALL BE TAKEN.**

The College's computer systems may be used only for College and progression-based activities, i.e. they are provided to support only the courses taught by the College and may be used only with the authorisation of the appropriate member of staff.

Note to Students Users: **Students whose accounts are suspended may find that it is impossible for them to complete their coursework.**

### 1. Scope

These guidelines apply to **ALL** users of the College's IT facilities and its cloud hosted systems, both in the College and when connected from off-site. The Computer Users' Code of Conduct protocols have been established in conjunction with TVCT's Online Safety and Email Policy.

### 2. Legal Requirements

2.1 Users of the College's computer equipment are subject to the provisions of the following regulations:-

- 2.1.1 The Data Protection Act, 2018
- 2.1.1 General Data Protection Regulations 2018
- 2.1.2 The Copyright, Designs and Patents Act, 1988.
- 2.1.3 The Computer Misuse Act, 1990.
- 2.1.4 The Telecommunications Act, 1984.
- 2.1.5 The JANET Acceptable Use Policy  
<https://community.jisc.ac.uk/library/acceptable-use-policy>
- 2.1.6 The Police & Criminal Evidence Act 1984
- 2.1.7 Regulation of Investigatory Powers Act 2000.
- 2.1.8 Counter-Terrorism and Security Act 2015

2.2 Offences against legislation may be investigated by the Police.

### 3. External Connections

The College network is a resource provided solely for **academic learning, training and research**. It is not provided for "social" use and access to the Internet may be removed from anyone using the network for inappropriate activities.

#### 4. The Use of College Equipment

- 4.1 Prior Pursglove and Stockton Sixth Form College provides and maintains its computing equipment and networks for the use of its staff, students and governors solely for educational teaching, administrative and research work.
- 4.2 Each user of the College's computer equipment must register as a computer user by submitting to the College a signed copy of the 'Computer Users' Code of Conduct'
- 4.3 Accounts will only be issued to people who have signed a copy of the 'Computer Users' Code of Conduct'.
- 4.4 Accounts will be made available to students soon after enrolment day and the accounts will remain active until the end of the Summer Term when they may be removed from the systems. Staff and governors accounts will be provided with an account which will last for the period of their employment/appointment.
- 4.6 Accounts on the College's systems are provided for use by the account owner only. Passwords should only be known by the account holder, and accounts should only be operated by the account holder.
- 4.7 Users must avoid leaving their computer unattended whilst logged on and the session is not locked. Users must be aware that in leaving their computer unattended that their personal data is vulnerable to interference and deletion by others. Users who have access to sensitive and personal data must not leave their computer unattended whilst logged on unless the session has been locked.
- 4.8 All requests for changes to a student's account will only be carried out on production of a valid College ID card.
- 4.9 Users shall not attempt to gain unauthorized access to college systems, data or accounts of other users.
- 4.10 Users shall not attempt to subvert network security, impair the functionality of the network or bypass restrictions set by network administrators. Users are also prohibited from destroying data by spreading computer viruses or vandalizing data, software or equipment.  
If a user violates any of the above it will be regarded as a very serious transgression of the Computer Users' Code of Conduct. This will result in immediate suspension of the user's access to the College's computing facilities. Further disciplinary action will follow – please see sections 13.1, 13.2 and 13.3.
- 4.11 Users must not use the college system to engage in: any other illegal act, arranging for a drug sale, purchasing alcohol for a minor, engaging in criminal activity, threatening the safety of a person, bullying, promotion of extreme political groups, extreme faith based religious groups and unethical or illegal views.
- 4.12 Users must not use the College's equipment to run software other than that provided by the College for use on the particular machine, except where they have written the software as an essential part of their coursework / work.
- 4.13 Users must not install, or attempt to install, any executable files on to the College's equipment without the appropriate authorisation from the Network Manager. This does not include compiling programs which users have written.
- 4.14 Equipment with which users suspect there is a problem should not be used, the problem should be reported to IT Support.

- 4.15 Student users will immediately notify a tutor if they identify a possible security problem (such as disclosure of their password to another person) and other users will immediately notify a member of the IT Support team. No users will go looking for security problems, because this may be construed as an illegal attempt to gain access.

## **5. Copyright**

- 5.1 Under no circumstances may any of the equipment at Prior Pursglove and Stockton Sixth Form College be used to make unauthorised copies of software or to run illegally obtained software. The network administrators must be in possession of a valid licence for all software that is used on (or copied on to) the network.
- 5.2 The College has entered into legal agreements for the use of the software on the computer networks. Copying, modification or unauthorised access of the software is prohibited.
- 5.3 Each user must respect the terms of all software licence agreements entered into by the College and shall accept personal responsibility for any deliberate breach of such agreements.
- 5.4 Each user must respect the copyright in all documentation and software made available by the College and shall accept personal responsibility for any violation of such copyright. Users will not plagiarise works that they find on the Internet. Plagiarism is taking the ideas or writings of others and presenting them as if they were original to the user.
- 5.5 Users will respect the rights of copyright owners and not infringe on those rights. Copyright infringement occurs when an individual inappropriately reproduces a work that is protected by a copyright. If a work contains language that specifies acceptable use of that work, the user should follow the expressed requirements. If the user is unsure whether they can use a work, they should request permission from the copyright owner.
- 5.6 All work produced on college equipment, software, and networks is the property of the Tees Valley Collaborative Trust.

## 6. Online Learning

- 6.1 Microsoft Office 365 is the preferred platform for conducting online learning and sharing of data and documents between users. Users should not use other platforms without permission from the Network Manager or Director of Resources.
- 6.2 Online sessions and meetings may be recorded – there will be an on-screen alert to let all participants know when recording is occurring. **Student users must not share, broadcast, or distribute recorded (video or audio) sessions to anyone.**
- 6.3 Attendees and organisers of online sessions (Microsoft Teams meetings and lessons) are responsible for following the General Data Protection Regulations (GDPR) 2018 and associated legislation. They must protect their own and others personal data. Disclosure of any personal data/information is to be avoided.

## 7. Quotas/Disk Space

- 7.1 User accounts on the College's network may have restricted disk space. If, in exceptional circumstances, student users require more disk space they should ask their teacher or tutor to apply on their behalf to the Network Manager with the appropriate justification. Staff users will need to make an individual request to the Network Manager.
- 7.2 Users will not download large files unless absolutely necessary. If necessary, users will download the file at a time when the system is not being heavily used and immediately remove the file from the system computer to their personal computer or diskette(s).

## 8. Electronic Mail (e-mail)

**The College has an e-mail policy which is part of the Computer Users' Code of Conduct and is included as an appendix in the paper-based version of this document. Users must adhere to the rules which are stated in the e-mail policy. The following are a brief summary of the key points.**

- 8.1 The College e-mail system may only be used for authorised purposes as defined in this policy.
- 8.2 The College retains the right to monitor and access users' e-mail systems if it has reasonable grounds to do so. The contents of users' e-mail will be accessed for:
  - security purposes;
  - for purposes of fulfilling legal requirements e.g. if a user is suspected of promoting extreme political views, extreme faith based religious views or unethical or illegal views;
  - for purposes of investigating/preventing a crime;
  - for ensuring effective operation of e-mail facilities;
- 8.3 Where the content of any accessed or retrieved e-mail contravenes any law, infringes the provisions of this e-mail policy or any other policy of this organisation, it will attract disciplinary actions.
- 8.4 IT facilities provided by the College for e-mail should not be used:
  - for the transmission of offensive material, unsolicited commercial or advertising material, chain letters, unauthorised press releases, or other junk mail of any kind, to other users, user organisations, or organisations connected to other networks

- for the unauthorised transmission to a third party of confidential material concerning the activities of Stockton Sixth Form College or Prior Pursglove College
- for the transmission of material such that this infringes the copyright of another person, including intellectual property rights

8.5 The College reserves the right to block any e-mail containing inappropriate or offensive language and to take action against any user sending such e-mails.

## 9. User Network Behaviour and the Working Environment

9.1 Users of the College's computing equipment must conduct themselves in a manner that promotes a productive working environment.

9.2 The College's equipment can only be maintained at an excellent standard with the help of all users. Users must report any faulty equipment - they should not tamper with it.

9.3 **Eating and/or drinking is not permitted in any of the computer rooms used for teaching purposes. All litter must be placed in the bins and the computer teaching rooms must be left in a clean and tidy state.**

9.4 The GDPR 2018 and Data Protection Act 2018 applies to all personal data stored on the College's computers. Each user must comply with the GDPR 2018 and Data Protection Act and any other legislation on the use of computer facilities. The user shall accept personal responsibility to register any use of personal data, to ensure that such use is covered by an entry in the Data Protection Register and to keep all data secure. Staff must comply with the College's Data Protection Policy.

9.5 Users must not display, transmit, send or print any message, data or other visible representation which is threatening, abusive or insulting to any person and likely to cause harassment, alarm or distress

9.6 Users will not knowingly or recklessly post false or defamatory information about a person or organization.

9.7 Users must not create, store, transmit or request to receive data which may be in breach of the Telecommunications Act, 1984 or contravenes the Counter-Terrorism and Security Act 2015 (Prevent Duty).

9.8 Users should not unnecessarily selfishly monopolise system resources.

9.9 Every user of the College's computing resources must respect other users. For example, large print jobs must be sent at off-peak times.

9.10 If a user cannot wait for a print job to complete it should be cancelled and reprinted later to allow others to access the printer. Print jobs not 'pulled' to a device will automatically cancel after a period of time (currently 4 hours).

9.11 Users must remove files from their directory which are no longer required.

9.12 Users should occasionally change their passwords and never leave them as the 'default' password. Passwords should contain upper case letters, lower case letters and numbers as a minimum level of complexity.

9.13 Users should never tell anyone their logon password. Note that this includes the technical support staff - if they require to logon to a user's account, they will ask for the password to be entered.

- 9.14 **Users must not logon to another user's account.**
- 9.15 If a software virus is detected, then users must report it to IT Support immediately.
- 9.16 All use of computer facilities should be identifiable. Failure of users to identify themselves with their ID and password may lead to the providers of some Internet services to withdraw them!
- 9.17 The network system will back-up users' files each night as part of the normal housekeeping process of the network.
- 9.18 All users are responsible for keeping their own back-ups of files not stored on the network.

## **10. Games**

- 10.1 Games are not permitted.
- 10.2 Users must not play, copy, store (in any format), or download games on the College's machines.

## **11. Safeguarding**

- 11.1 Users should take steps to ensure their comfort and health whilst using computers by: taking regular breaks away from the computer; adjusting the height of the chair; avoiding glare on screens by closing blinds in sunny weather.
- 11.2 Users must not engage in any harassment or cyber bullying, including over the computer network.
- 11.3 Users must take steps to safeguard themselves from harm when using computers. Personal information should not be posted where strangers could gain access to it.

## **12. Additional Hardware**

- 12.1 Users must not connect their own peripheral devices to the College's machines without seeking permission from IT support first. The only exception is that users are allowed to connect their personal stereo headphones to the front of the Computers using the jack socket where provided.
- 12.2 All equipment must have been tested for electrical safety before it is connected to the College's equipment.

## **13. Privacy of Files**

- 13.1 The college will monitor students' online activities especially if they are suspected of violating the Computer Users' Code of Conduct or the law (e.g. The Computer Misuse Act, 1990; The Telecommunications Act, 1984. The Police & Criminal Evidence Act 1984; The Counter-Terrorism and Security Act 2015). The college also reserves the right to monitor other users (e.g., non-students) online activities.
- 13.2 The college reserves the right to employ and review the results of software that searches, monitors and/or identifies potential violations of the Computer Users' Code of Conduct.
- 13.3 Users should be aware that their personal files may be disclosed in court and administrative proceedings.
- 13.4 System users have no privacy expectation in the contents of their personal files and records of their online activity while on the college systems.

## 14. Penalties and access privileges

14.1 These guidelines are designed to prevent avoidable network problems and to ensure that the College's networks are kept secure and efficient. Violation of these guidelines will lead to the suspension of the user's account and the matter will be reported to the Principal who will determine the disciplinary action which shall be taken.

14.2 The college may revoke Internet access at its sole discretion. If a student's access is revoked, the college will ensure that the student nonetheless continues to have a meaningful opportunity to participate in the educational program.

**Note to Student Users - Students whose accounts are suspended may find that it is impossible for them to complete their coursework.**

14.3 Employee violations of the college Computer Users' Code of Conduct will be handled through the appropriate disciplinary procedures.

14.4 The college will cooperate fully with police and government officials in any lawful investigation concerning or relating to any illegal activities conducted through the college system.

14.5 **Users are responsible for their own accounts.** If someone else misuses an account, the account owner could be subject to the penalties outlined above.

14.6 All members of the college are expected to be responsible users of computers. There may however be times when infringements of the policy could take place, through carelessness, lack of understanding, SEN, and irresponsibility.

14.7 Incidents of misuse will be investigated in conjunction with the protocols of TVCT's Online Safety Policy to determine the cause of the breach of the code of conduct. If there are mitigating circumstances as to the cause of the misuse of computer usage these will be considered as part of the investigation.

Where the misuse relates to filtering or security breaches, or use of sites which should be filtered, the IT Manager will notify and report to the Senior Leadership Team at the college in line with the requirements of Keeping Children Safe in Education 2023 and the filtering and monitoring standards published by the Department for Education.

Date of Last Approval/Revision	July 2023
Review interval (years)	Yearly
Responsible Officer	Director of Resources
Approval/review body (ies)	SLT
Date of next review	July 2024

This policy has been subject to an Equality Impact Assessment by:

Author/Reviewer: Director of Resources

SLT/EET: SLT July 2023