KING EDWARD VI COLLEGE
STOURBRIDGE

Policy Document

Computer Misuse

1 Introduction

This policy and its supporting documentation sets out the way in which students, staff and governors should use college computers, phones, tablets, applications and the associated network infrastructure (including Wi-Fi) and has been drawn up to protect all parties.

2 Policy

All users of computer facilities at King Edward VI College are required to agree:

a) A statement of their responsibilities in respect of the use of college IT equipment, which enables the college to enforce any necessary action; and
b) To abide by the conditions of use as indicated in the supporting documentation

3 Policy Guidelines

a) Students are required to make this undertaking by signing their learning agreement
b) Staff and governors are required to sign a copy of the acceptable use statement when they take up their employment or governance duties at the College, or when they are first in receipt of a college device
c) This undertaking includes an agreement to comply with the statutory and other provisions and regulations applicable to computer systems and the information stored in them.

4 Supporting Documentation

Annex 1. Computer conditions of use
Annex 2. Acceptable use agreement for staff and governors
Annex 3. Acceptable use agreement for students

5 Equality Impact

The College's equality, diversity and inclusion policy has been taken into account when considering this policy. The College will provide reasonable adjustments, including assistive technologies, to ensure all users can access IT systems fairly.

Date of review	Date agreed	JCC	Governors	Review date	Comments
September 2025	December 2025	25/09/2025	N/A	October 2026	

Computer Conditions of Use Annex 1

1. General requirements for good practice

1.1 Computing resources, such as workstations, laptops, phones and tablets, printers, email and Wi-Fi, and any other part of the College computing systems, must only be used for research, teaching, coursework, governance, or associated administration purposes and for legitimate private interests. This extends to the use of personal devices which access the college's Wi-Fi system. These devices must not be used for illegal activity (such as hacking or Intellectual Property violations), nor to display, store or transmit text or images that could be considered offensive, for example material of a sexual, pornographic, racially offensive or abusive nature. Contravention of these rules may also be an offence under the Computer Misuse Act 1990, the Obscene Publications Act or the Equality Act 2010.

1.2 In particular, the access of and sharing of materials that may be considered as contributing to radicalisation is expressly forbidden. Any such breach will be reported to the relevant authorities under the Prevent strategy. This may also be an offence under the Counter-Terrorism and Security Act 2015.

1.3 Appropriate action will be taken against offenders. The college may be obliged to inform the authorities about any apparent breach of the law. If you are in any doubt as to what constitutes acceptable computing behaviour, please contact the IT Manager.

1.4 King Edward VI College will require restitution for any theft of computing resources and for any cost incurred due to misuse.

1.5 Software made available on the Company Portal may be installed on college owned devices without requiring prior permission. Any other software installations must take place under the direction of the IT Manager.

1.6 Proprietary software must be installed in conformity with its licence agreement.

1.7 Unauthorised software and/or data must not be loaded or run on any computer - the IT Manager will advise on the acceptability for College use of software and data.

1.8 No 'non-educational' software is to be installed on college owned or managed computer equipment. Appropriateness of software must be checked with the IT Manager prior to any installation.

1.9 Harassment through any electronic means (including Teams messaging tools, social networking sites, email, software manipulation) is expressly forbidden.

1.10 The college reserves the right to inspect and delete users' files or messaging logs without prior notice to ensure compliance with the policy and applicable laws should the need arise. Authorisation is given by the Principal or their delegated SLT member.

1.11 Telephone calls are not listened into or recorded by the College.

1.12 Telephone usage may be monitored on a monthly basis, on the basis of cost, duration, frequency or other inappropriate use (e.g. overseas, premium rate lines)

1.13 As a result of this monitoring, individuals may be contacted for clarification of use.

2 Viruses

2.1 All machines have virus-checking software installed. If a virus is detected, or suspected, users must contact the IT Services staff immediately.

2.2 Following the growth of 'ransomware' attacks, users should be suspicious of emails from all sources (known or otherwise), especially those containing unexpected attachments, or links to 'log-in' pages. All suspicious emails should be forwarded to helpdesk@kedst.ac.uk.

2.3 All removable storage must be encrypted and virus checked before use. All internet downloads must be actioned from reputable sites, and be virus checked prior to opening.

2.4 Any queries about viruses contact the IT Services staff.

3 Compliance with the requirements of legislation

There are four Acts that apply directly to all computing systems in the college

3.1 Computer Misuse Act

3.1.1 In essence this Act makes it an offence to access, or to try to access, any computer system for which access authorisation has not been given. Thus any attempt to interfere with, or try to bypass, the security controls on a computing system is an offence. Similarly, trying to obtain information, such as other users' passwords or accessing or modifying files belonging to other people who have not given access authorisation is also an offence. All such offences are known as "Section 1 offences". The maximum penalty for this offence is 2 years imprisonment.

3.1.2 An unauthorised access offence, which is committed with the intention of committing or enabling the commission of other offences, is more serious, as is the unauthorised modification of computer material. These offences are known as "Section 2 offences", and carry a maximum penalty of 5 years in prison.

3.1.3 An unauthorised access offence committed knowing it to be unauthorised and is later considered to be 'reckless' are known as "Section 3 offences". Depending upon whether they can cause harm to human welfare or national security, these offences can carry a maximum penalty of between 14 years and life imprisonment.

3.2 Copyright, Design and Patents Act

This Act makes it an offence to copy documentation or software without the permission of the owner of the copyright. It applies to all software in use in the college. The college will take severe action against any person found to be copying or to have copied without permission software for which the college holds a licence. Breaches of this Act can also lead to legal action.

3.3 UK GDPR and Data Protection Act 2018

In general, this Act requires that all personal data relating to other living persons, with exception of personal data held by an individual for domestic and recreational purposes, should not be stored by any person on a computer system in the college unless the data is suitably registered. The Data Protection Lead should be consulted if the need to store such data is thought to have arisen.

3.4 Counter Terrorism and Security Act

This act sets expectations on a College to monitor access to equipment, websites and other material which promotes terrorism or violent extremism or which seeks to radicalise individuals to these causes. This may also require the College to monitor communications where activities of this nature are suspected.

3.5 Online Safety Act

This act places legal responsibility on tech companies to prevent and rapidly remove illegal content and aims to stop children seeing material that is harmful to them.

3.6 Artificial Intelligence Tools

The use of generative AI tools (e.g. ChatGPT, Copilot, Gemini) must comply with the College's academic integrity and safeguarding requirements. Users must not input confidential student, staff, or college data into external AI platforms.

4. Conclusion

4.1 The user is responsible for ensuring that their activities (or lack of activity) do not expose the college to any of the above.

4.2 By signing the Acceptable Use Statement and/or the learner agreement, the user agrees to comply with the policy and conditions of use.

4.3 Breaches of this policy may result in withdrawal of IT access, disciplinary action up to dismissal (for staff/governors) or exclusion (for students), and referral to the police or other authorities where a criminal offence is suspected.

Purpose

This agreement summarises the key responsibilities and required behaviour of ***all*** staff and governors of King Edward VI College, Stourbridge in use of College computer and information systems.

Background

The telecommunication and computer system is owned by the College and is made available to staff and governors to execute their duties efficiently and effectively.

The College's policy on Computer Misuse has been drawn up to protect all parties – the staff, governors, students and the College.

The Acceptable Use Agreement is framed by UK Legislation and guidance including:

- Computer Misuse Act 1990
- UK GDPR and Data Protection Act 2018
- Counter Terrorism and Security Act 2015
- Prevent duty guidance: England and Wales 2023
- Freedom of Information Act 2000
- Investigatory Powers Act 2016
- Keeping children safe in education 2023
- Online Safety Act 2023

Breaches of the agreement and conditions of use will result in appropriate disciplinary action being taken against the offender in accordance with the Staff Disciplinary Procedure or appropriate action in accordance with the governors' rules and standing orders and adherence to the code of conduct.

Rules

General

1. With the exception of mobile devices supplied to staff and governors for their use, computer equipment must not be removed from College without permission from the appropriate College Senior Leader;
2. With the exception of approved software available on the Company Portal, staff and governors must not install software on College computers, servers and laptops;
3. Staff and governors must not circumvent any security measures put in place on college owned devices to ensure the safe operation of computing equipment, information systems of communications equipment e.g. disabling anti-virus software, removing password protections etc;
4. Staff and governors must take account of their working area and ensure that no one's personal data is viewable to those who have no reasonable purpose in seeing it;
5. Staff and governors must adhere to the terms and conditions of all licence agreements relating to any software installed on, or accessed by, College devices including restrictions for commercial use;
6. Staff and governors may only access, modify, save or copy records or files and computer records where you have been given the authority to do so;

7. Staff and governors must ensure that all processing of personal data is in accordance with the college's privacy notices;
8. Staff and governors must not connect personal equipment to the College's wired network without permission from the IT Manager;
9. Staff and governors must comply with the JANET network Acceptable Use Policy when using an internet connection from or to the College, including:
    - Not engaging in harassing, defaming or other anti-social behaviours on-line
    - Not creating or transmitting any offensive, obscene or indecent images, data or other material in any form
    - Not using the network to attack or gain unauthorised access to other network, computer systems or data
    - Not transmitting unsolicited bulk email (spam)
    - Not infringing the copyright of another person or organisation
10. Staff and governors must ensure unattended computers and laptops are "locked" and that they log out of College systems at the end of each session;
11. Staff and governors must ensure personal devices such as smartphones with access to college software or services have appropriate protection against viruses and are secured with a login password, passcode, security pattern, or biometric details such as fingerprint or facial recognition;
12. Staff and governors must report all potential data breaches or concerns to the College's Data Protection Lead immediately they become aware of an issue.

Telephone Communication

1. Telephone calls are not listened to or recorded by the College, but telephone usage may be monitored on a monthly basis identifying cost, duration and frequency of calls

Your IT Account

1. Access must only be made via the authorised account and password, which must not be made available to any other person;
2. Activity that threatens the integrity of the College's ICT systems, or that attacks or corrupts other systems, is strictly forbidden;
3. Backups of central storage areas (online and local) is taken for disaster business purposes only and users must back up their own personal work through other means. If you are unsure how to do this, speak to the IT Manager;

Sensitive Data Protection

1. Staff and governors must ensure that personal data is stored in an authorised and secure file system. An annual audit will be conducted by the Data Protection Lead;
2. Home computers, laptops, smartphones and other devices that can access the college network remotely must be suitably secured to prevent anyone other than the member of staff or governor from accessing college data, software or services;
3. Do not pass any student data to a third party without the student's agreement or the Data Protection Lead's permission. Any data that is shared must be done so securely. If you are unsure how best to do this, speak to the Data Protection Lead.

Interception and Examination of Files

1. The College reserves the right to examine or delete any files that may be held on its computer systems;
2. The College does not actively monitor the contents of emails, communications or file spaces. The College does monitor for abnormal network traffic, spam, malware and patterns that may indicate misuse or unauthorised access. The College has a procedure for authorised investigations e.g. arising from a complaint, and where necessary reserves the right to investigate all information stored on College systems and services, including email and Teams messaging tools;
3. The College has a duty to allow UK law enforcement agencies to access your College email account and central storage (online and local) where a warrant/request is properly executed in relation to an investigation;

Infringement of Copyright

1. Copyright of materials and intellectual property rights must be respected in accordance with the College's Plagiarism Policy;
2. No copyright DVDs, CDs or other material may be copied using College computer equipment;
3. Staff and governors must not submit or post copyright material, without permission, to College forums, blogs and web sites;

Creation or Upload of Unacceptable Material

1. Staff and governors are not allowed to take photographs, videos or recordings of any members of the College community without the full permission of all those appearing in the images or recordings, and in most cases, prior permission of their parents/guardians;
2. Staff and governors are not allowed to post on web sites or distribute material, including images, videos or recordings, which brings the College or its employees or students into disrepute.

Use of College Email and other online College communication systems and resources

1. Staff and governors are responsible for all emails, texts or communication via other messaging services and for contacts made that may result in these digital communications being received;
2. Digital communication-based conversations containing personal information can be requested and made available to the person it is about under a GDPR 'Subject Access Request'. Ensure all your communications use professional language, are fair, accurate and justifiable.
3. Digital communication-based messages are confidential and intended solely for the use of the individual to whom they are addressed; any use, dissemination, and forwarding, printing or copying of emails of text messages by third-parties without permission is strictly prohibited;
4. Mass messages to large numbers of individuals can only be sent with the authority of a member of the College Leadership Team;
5. Staff and governors must not submit or post material that is harassing, libellous, abusive, threatening, harmful, vulgar, obscene or otherwise objectionable in any manner to College forums, blogs, web sites or messaging tools.
6. Staff and governors must not impersonate other individuals when they submit or post material to College forums, blogs, web sites or messaging tools;

7. Staff and governors must not submit or post advertisements or commercial solicitations to College forums, blogs, web sites or messaging tools;
8. Any information, opinions or other content provided on College forums and blogs is for educational purposes only;

Use of Mobile Devices

1. Staff and governors must take additional care when using College, or personal mobile technologies to hold College data (including email) or access systems. You must ensure that your device is secured and protected from interference;
2. Staff and governors may connect personal devices to the College wireless network. While connected to College Wi-Fi through a personal device they and their devices are subject to the terms and conditions laid out in this policy;
3. Staff and governors must ensure that any device they connect to the College Wi-Fi network is free from malicious code;

Use of Social Media

1. Staff and governors should ensure that any social media accounts they have are set up with the appropriate privacy controls to ensure posts they make, or that are made to their accounts are seen only by intended recipients;
2. Staff and governors must ensure that any social media post (Facebook, 'X' (formally known as Twitter), Instagram, Tik-Tok, blogs, forums etc) they make does not bring themselves, the College, staff, governors, or students of the College into disrepute; posting links to websites which express extremist views or include inappropriate material may result in appropriate action being taken and the relevant authorities informed where applicable under the college's Prevent Strategy.
3. Cyberbullying of any kind is not tolerated by the College. Instances of such behaviour can and have led to actions similar to those detailed above.

I have read and understood the contents of this acceptable use agreement.

Name [print]:

Signature: Date:

Acceptable Use Agreement for Students Annex 3

Purpose

This agreement summarises the key responsibilities and required behaviour of ***all*** students of King Edward VI College, Stourbridge in use of College computer and information systems.

Background

The telecommunication and computer system is owned by the College and is made available to students to further their education. All students will be required to sign a copy of the agreement if they wish to use College telecommunications, computer systems and machines. Any student wishing to have further guidance on the agreement before they sign should see their Personal Tutor.

The College's policy on Computer Misuse has been drawn up to protect all parties – the staff, governors, students and the College.

The Acceptable Use Agreement is framed by UK Legislation including:

- Computer Misuse Act 1990
- UK GDPR and Data Protection Act 2018
- Counter Terrorism and Security Act 2015
- Prevent duty guidance: England and Wales 2023
- Freedom of Information Act 2000
- Investigatory Powers Act 2016
- Keeping children safe in education 2023
- Online Safety Act 2023

Breaches of the agreement and conditions of use will result in appropriate disciplinary action being taken against the offender in accordance with the Student Management Policy.

Rules

General

1. Students must not remove computer equipment from College without permission from the appropriate member of the College Leadership Team;
2. Students must not install software on College computers, servers or laptops. Software may be installed on college owned mobile devices but only under the direction of a member of staff;
3. Students must not circumvent any security measures put in place to ensure the safe operation of computing equipment, information systems of communications equipment e.g. disabling anti-virus software, removing password protections etc;
4. Students must adhere to the terms and conditions of all licence agreements relating to any software installed on, or accessed by, College computers including restrictions for commercial use;
5. Students may only access, modify, save or copy records or files and computer records where they have been given the authority to do so;
6. Students must not connect equipment to the College's wired network without permission from the IT Manager;

7. Students must comply with the JANET network Acceptable Use Policy when using an internet connection from or to the College, including:
    - Not engaging in harassing, defaming or other anti-social behaviours on-line
    - Not creating or transmitting any offensive, obscene or indecent images, data or other material in any form
    - Not using the network to attack or gain unauthorised access to other network, computer systems or data
    - Not transmitting unsolicited bulk email (spam)
    - Not infringing the copyright of another person or organisation
8. Students must ensure that unattended computers and laptops are "locked" and they log out of College systems at the end of each session;

Your IT Account

1. Access should only be made via the authorised account and password, which should not be made available to any other person;
2. Activity that threatens the integrity of the College's ICT systems, or that attacks or corrupts other systems, is both strictly forbidden and illegal, and can result in a prison sentence;
3. Backups of network drives are taken for disaster recovery purposes only and users must back up their own important work through other means.

Interception & Examination of Files

1. The College reserves the right to examine or delete any files that may be held on its computer systems;
2. The College does not actively monitor the contents of emails, communications or central storage areas. The College does monitor for abnormal network traffic, spam, malware and patterns that may indicate misuse or unauthorised access. The College has a procedure for authorised investigations e.g. arising from a complaint, and where necessary reserves the right to investigate all information stored on College provided systems and services, including email;
3. The College has a duty to allow UK law enforcement agencies to access your College email account and central storage areas where a warrant/request is properly executed in relation to an investigation.

Infringement of Copyright

1. Copyright of materials and intellectual property rights must be respected in accordance with the College's Plagiarism Policy;
2. No copyright DVD's, CDs or other material may be copied using College computer equipment;
3. Students must not submit or post copyright material, without permission to social media of any kind, or forums, blogs and other web sites;

Creation or Upload of Unacceptable Material

1. Students are not allowed to take photographs, videos or recordings of other students or College employees without the full permission of all those appearing in the images or recordings, and in most cases, prior permission of their parents/guardians;

2. Students are not allowed to post on social media or web sites, or distribute material, including images, videos or recordings, which brings the College or its employees or students into disrepute;

Use of College Email and other online College communication systems and resources

1. Students are responsible for all emails, texts or communication via other messaging services and for contacts made that may result in these digital communications being received;
2. The same professional level of language and content should be applied as for letters or other media, particularly as emails or texts are often forwarded;
3. Digital communication-based messages are confidential and intended solely for the use of the individual to whom they are addressed; any use, dissemination, forwarding, printing or copying of emails of text messages by third-parties without permission is strictly prohibited;
4. Mass messages to large numbers of individuals can only be sent by a member of the College Leadership Team;
5. Students must not submit or post material that is harassing, libellous, abusive, threatening, harmful, vulgar, obscene or otherwise objectionable in any manner to social media of any kind, or forums, blogs and other web sites;
6. Students must not impersonate other individuals when they submit to social media of any kind, or forums, blogs and other web sites;
7. Students must not submit or post advertisements or commercial solicitations to social media of any kind, or forums, blogs and other web sites;
8. Any information, opinions or other content provided on College systems, forums and blogs is for educational purposes only;

Use of Mobile Devices

1. Students must take additional care when using College, or personal mobile technologies to hold College data (including email) or access systems. You must ensure that your device is secured and protected from unauthorised access;
2. Students may connect personal devices to the College wireless network. While connected to College Wi-Fi through a personal device, students and their devices are subject to the terms and conditions laid out in this policy;
3. Students must ensure that any device they connect to the College Wi-Fi network is free from malicious code;

Use of Social Media

1. Students should ensure that any social media accounts they have are set up with the appropriate privacy controls to ensure posts they make, or that are made to their accounts are seen only by the people the student intends;
2. Students must ensure that any social media post (Facebook, ‘X’ (formally known as Twitter), Instagram, TikTok, blogs, forums etc) they make does not bring themselves, the College, staff or students of the College into disrepute; posting links to these services which express extremist views or hold inappropriate material may result in serious disciplinary action being taken and the appropriate authorities informed where applicable under the college’s Prevent Strategy.
3. Cyberbullying of any kind is not tolerated by the College. Instances of such behaviour can and have led to students’ permanent exclusion.