Godalming College

IT Acceptable Use & E-Safety Policy (Students)

Learning together for success and progression

IT Acceptable Use Policy & E-Safety (Students)

Introduction and Purpose

- The College seeks to provide a consistently outstanding, stable and secure IT network for all College users at all times
- The College expects all users of College IT systems to use them appropriately
- The College also has a statutory duty, under Section 26 of the Counter Terrorism and Security Act 2015, termed 'PREVENT'. The purpose of this duty is to aid the process of preventing people being drawn into terrorism
- This Policy is to protect the College IT systems from intentional or unintentional abuse
- To uphold the legal responsibility on the part of the College to ensure that all users of College IT systems work within the requirements of the relevant Acts, Regulations and Laws
- To try to prevent any activity on College IT networks that could bring the College into disrepute or cause financial or legal penalties
- To make users aware, thorough this policy alongside the Student Code of Conduct, and other related procedures, of their individual responsibilities to ensure that they do not do anything on the College IT Systems that would conflict with this Policy

Scope

The Policy is for all students at the College

Section One: Network Use and Security

1.1 Network Security

Any User of the College network must be a currently registered User with a designated ID to use the Godalming College network.

A User must:

- Keep your login details private and secure -they must not be given to anyone
- Be respectful to others
- Look after College IT equipment
- Take reasonable precautions to ensure all personal equipment you use to connect to the College is kept up-to-date (e.g. daily updates) and is free from viruses or spyware and is secure

A User must not:

- Reveal their network password to anyone or allow any other use to use a machine that is logged in under their name
- Use any ID which is not their own, or use a machine which is logged in under an ID that is not theirs
- Corrupt, destroy or violate the privacy of another user's data or work
- Introduce viruses or other disruptive elements to the system
- Use encrypted files, unless prior permission is obtained and the passwords/keys have been made available to a member of the IT department
- Use College resources in a way which is disruptive to others

1.2 Network Usage

The Godalming College IT Network and resources are there to create, view and transmit work relating to your College role. Network access rights and saved files will automatically be deleted when you leave.

You must NOT use the College IT Network and computing resources for the creation, viewing or transmitting of any images, literature or data that is:

- Offensive, obscene, indecent, or inflammatory
- Designed to or likely to cause annoyance, inconvenience or anxiety e.g. bullying or harassment
- The copyright of another person
- Unsolicited commercial or advertising material

Any such use is likely to result in Disciplinary action.

1.3 User Area Drive Capacity

A User Area Capacity will be set by the College to limit the size of files that an individual can save onto the server. Each user is responsible for the content and maintenance of their user area.

1.4 Systems and Software Security

- Users may only use applications preinstalled on the network, workstation or College issued device
- Wherever possible users should avoid using USB Memory Cards, and they must never be used to store Personal Information (information relating to people)
- Users should not interfere with hardware or software configurations of any systems or equipment
- Users must not download or use any additional software not authorised by the College IT Team (including games or .exe)
- Users must not download to the network, any image, music or large files unless related to College work
- Users must not download or use any copyrighted material, without written consent from the copyright holder

2. Internet, E-Mail and Social Media Use

2.1 Internet Use

Users may not access, encourage access or disseminate materials which the College deems to be obscene, pornographic, excessively violent, offensive or that acts as an incitement to criminal behaviour. Internet access for all purposes is reviewed regularly by the IT Department. The College may exercise its right to monitor the use of its computer systems, including the monitoring of websites, the interception of e-mails and the deletion of inappropriate materials where it believes the College's computer system is being used inappropriately. All users have prescribed internet permissions that apply whilst accessing the Internet through any device.

In line with our aim to keep students safe from radicalisation and exposure to terrorist and extremist or potentially distressing material, the College additionally monitors and reports on related online activity. The level of monitoring and filtering is under constant review. The College Safeguarding Team is responsible for the monitoring.

Unknown websites are blocked by default but can be requested via the IT Department.

2.2 Internet Filtering

- All users of the College network have their internet use automatically monitored and a record of sites visited is recorded by the College IT Team. This information can be used in the event of disciplinary proceedings.
- The College provides user-based internet filtering, allowing an appropriate level of browsing permission, following the guidance from the DfE's KCSIE document. The following are examples of blocked categories: Proxy Avoidance, Gambling, Nudity, Spam, Drugs, Dating, Illegal, Radicalisation, Weapons, Hate, Racism, Violence
- Internet use which is detected as posing a risk is automatically reported to the College Safeguarding Lead for investigation
- Websites and services are reviewed individually from permitted categories such as social media, entertainment, streaming media and instant messaging. Additional controls may be imposed at any time
- All Users must adhere to internet controls in place and no attempts to bypass them are permitted. Services such as VPNs (Virtual Private Networks) and Proxy Servers are not permitted on the College network
- In the event of accidental breach, please seek the immediate guidance and support of the IT Department

2.2 E-mail usage

E-mail is a widely used and valuable function within any professional organisation. It is recognised as a key vehicle of communication for the College both internally and externally.

Where messages are private and personal, a private e-mail account is the most appropriate vehicle to be used.

The College expectation is that e-mails should be checked by students at least every 24 hours during term time (excluding holidays).

E-mail by its very nature is not secure or confidential. Messages can be seen by other people. Do not put in anything in a message that should not be seen by everyone. It is the user's responsibility to ensure that communications that are sent do not involve the College in any potentially embarrassing or libellous situations. Legally, the laws of libel apply.

College e-mail accounts are not private and the College has the right to access them. Students should be aware that e-mail messages sent from or to a College e-mail account can inform or be the basis of disciplinary action.

- Users should be mindful of opening e-mails from unknown or untrusted sources
- Users should delete emails as soon as they are no longer needed

2.3 Social Media

The term "Social Media" encompasses social networking sites such as, but not limited to, Facebook, Instagram, WhatsApp, Snapchat and Twitter, as well as to more general types of social media and instant messaging such as, but not limited to, blogs, wikis, podcasts and digital images/videos.

Every individual is legally liable for anything they write or present online. Students can be disciplined for any commentary, content or images that are viewed as defamatory, pornographic, and harassing.

Students should be mindful that what they publish could be publicly available indefinitely. Universities and future employers could access even your earliest posts on social media. Publishing any material that defames the College will always be dealt with as a serious disciplinary matter.

Students must:

- be conscious of the need to maintain the terms and conditions of their Student Contracts when using Social Media, specifically the obligation: *To be responsible and considerate in and out of lessons, always showing respect to all members of the College community, as well as to members of our local community.* In this instance the community also includes the online community
- not engage in activities involving social media which might bring the College into disrepute
- not represent personal views as those of the College
- not discuss personal information about other students or staff
- not use social media and the internet in any way to attack, insult, abuse or defame fellow students, staff, their family members or the College
- not use College email addresses and other official contact details must not be used for setting up personal social media accounts or to communicate through such media
- not use or publish the College corporate logos or brands on personal web space
- speak to the Assistant Principal Safeguarding and Support or Director of Marketing if they wish to set up social media site for a College enrichment group. Failure to do so could result in disciplinary action

3. E-Safety

Students must:

- ask a member of the IT staff if they are not sure if something is allowed
- make sure that my internet is safe and legal
- be aware that actions online have offline consequences. For more information look at:
    - https://saferinternet.org.uk
    - https://www.thinkuknow.co.uk
    - https://nationalonlinesafety.com
- be aware that people online are not always who they say they are and that I must always talk to an adult e.g. parent/carer, before meeting any online contacts
- know that people met online may not be who they say they are. If the adult deems it safe to meet this person, you should always meet in a public place with a trusted adult present
- speak to an adult I trust if something happens to either myself or another student which makes me feel worried, scared, or uncomfortable
- check my privacy settings with an adult to make sure they are safe and private and not share my passwords with anyone
- think before sharing personal information and always seek advice from an adult if unsure
- understand that the College internet filter is there to protect students, and not try to bypass it
- understand that bullying in any form (on and offline) is not allowed and that technology should not be used for any form or abuse or harassment
- always check that any information used online is true and accurate
- not upload or add any images, video, sounds or text that could upset, threaten the safety of or offend any member of the College community
- always think before posting as text, photos or videos can become public and impossible to delete
- not use technology to be unkind to others
- only upload appropriate pictures or videos of others online when I have their permission
- know cybercrime can be a criminal offence, for example gaining unauthorised access to systems ('hacking') and making, supplying or obtaining malware

- understand it can be a criminal offence to send threatening and offensive messages
- respect other people's information and copyright by giving a reference and asking permission before using images or text from online sources
- understand that it may be a criminal offence or against the rules of the College policy to download or share inappropriate pictures, videos, or other material online
- write emails and online messages carefully and politely as they could be forwarded or seen by someone who is not the intended audience
- report it to a member of staff immediately anyone trying to misuse technology
- respect the College internet access and equipment; students failing to do so will lose the right to use them
- not access or change other people's files, accounts, or information nor advertise anything on College IT systems
- understand that if the College suspects inappropriate behaviour with technology, it will be investigated
- be aware that personal devices e.g. Laptop/iPad may be inspected and/or confiscated

To find out more about keeping safe online students can visit:

- www.thinkuknow.co.uk
- www.childnet.com,
- www.childline.org.uk
- https://nationalonlinesafety.com

4. Related Documents

Internal:

- Student Code of Conduct
- Data Protection Policy
- Child Protection and Safeguarding Policy
- Equality, Diversity and Inclusion Policy
- Whistleblowing Policy

External:

- Counter Terrorism and Security Act (2015)
- The Human Rights Act 1998
- The Computer Misuse Act 1990
- The Data Protection Act 1998
- Libel Act 1843
- Defamation Acts 2013
- JANET Acceptable Use Policy
- JANET Security Policy
- Keeping Children Safe In Education 2016 (to most recent)
- Obscene Publications Act 1959 & 1964
- Protection of Children Act 1999
- Telecommunications Act 1984
- Protection from Harassment Act 1997
- Criminal Justice Act 2003
- Malicious Communications Act 1998
- Communications Act 2003
- Copyright and Related Rights Regulations 2003