ACCEPTABLE USE POLICY (STAFF)

2021

Carl Rusby (Senior Leader for ILT Strategy)
April 2021

Aim

As an educational institution with responsibility for safeguarding, it is important that staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. All members of staff have a responsibility to use the college's computer systems in a professional, lawful, and ethical manner. To ensure that members of staff are fully aware of their professional responsibilities when using technology, they are asked to read this Acceptable Use Policy.

Scope

This policy applies to all staff within the college environment who have access to the college IT systems, both on the premises and remotely. This policy applies to the use of all technology including college and personal devices.

This Acceptable Use Policy is taken to include the JANET Acceptable Use Policy (https://community.jisc.ac.uk/library/acceptable-use-policy) and the JANET security Policy https://community.jisc.ac.uk/library/janet-policies/security-policy published by JANET (UK).

Keeping children safe in education guidance means the College has a statutory duty to carry out appropriate filtering and monitoring. The College also has a statutory duty, under Section 26 of the Counter Terrorism and Security Act 2015, termed "PREVENT", to aid the process of preventing people being drawn into terrorism.

Any user of college IT systems are required to adhere to the agreed policy and regulations and to abide by the relevant policies for staff conduct.

Acceptable Use Policy Statements and Terms

Although this is not an exhaustive list; all members of staff are reminded that IT use should be consistent with the college ethos, college policies, national and local guidance and expectations, and the Law.

1. I understand that Information Systems and IT include networks, data and data storage, online and offline communication technologies and access devices. Examples include laptops, mobile phones, tablets, digital cameras, email and social media sites**.**

2. College owned information systems must be used appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.

3. I understand that any hardware and software provided by my workplace for staff use can only be used by members of staff and only for educational use. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate. I will protect the devices in my care from unapproved access or theft.

4. I will respect system security and will not disclose any password or security information. I will use a 'strong' password to access college systems. A strong password has numbers, letters and symbols, with 8 or more characters, does not contain a dictionary word and is only used on one system. I agree to use multi-factor authentication (MFA) where installed to access college systems securely.

5. I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without agreement from staff in IT support.

6. I will ensure that any personal data of students, staff or parents/carers is kept in accordance with the Data Protection Act 2018 (including GDPR).
    - This means that all personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online or accessed remotely.
    - Any data being removed from the college site (such as via email, cloud storage or on memory sticks or CDs) will be suitably protected. This will include data being encrypted by a method approved by the college where sensitive or personal information is involved.
    - Any devices taken off-site that may hold personal or sensitive data relating to College business must be encrypted.

7. I will not keep documents which contain college-related sensitive or personal information, including images, files and videos, on any personal devices, such as laptops, digital cameras, and mobile phones. If I wish to use college email on my personal device I agree to the terms and conditions. I will use any remote access services to retrieve any work documents and files in a password protected environment.

8. I will not store any personal information on the college computer system including any college laptop or similar device issued to members of staff that is unrelated to college activities, such as personal photographs, files, emails or financial information. I understand that if I do this it may be seen by subsequent users of the device.

9. I will respect copyright and intellectual property rights and understand that work produced whilst carrying out my duties at college remains the property of college.

10. I have read and understood the college eSafety (staff) policy which covers the requirements for safe IT use, including using appropriate devices, safe use of social media and the supervision of students within the classroom and other working spaces.

11. I will immediately report any illegal, inappropriate or harmful material or incidents I become aware of, to the Designated Safeguarding Lead.

12. I will not attempt to bypass any filtering and/or security systems put in place by the college. If I suspect a computer or system has been damaged or affected by a virus or other malware I will report this to the IT Helpdesk as soon as possible. If I suspect any college related documents or files may have been accessed by another individual or I am no longer in possession of this data (e.g. as a result of theft or loss) I will report this to the Data Protection Officer in MIS immediately in line with the data protection policy and procedures.

13. My electronic communications with current or past students, parents/carers and other professionals will take place within clear and explicit professional boundaries and will be transparent and open to scrutiny, should the need arise.
    - All communication will take place via college approved communication channels, such as a college provided email address or telephone number, and not via my personal devices or communication channels, such as personal email, social networking or mobile phones.
    - Any pre-existing relationships or situations that may compromise this will be discussed with the Designated Safeguarding Lead and/or Principal.

14. I will ensure that my online reputation and use of IT and information systems are compatible with my professional role, whether using college or personal systems. This includes the use of email, text, social media, social networking, gaming and any other devices or websites.
    - I will take appropriate steps to protect myself online as outlined in the eSafety (staff) policy and will ensure that my use of IT and the internet will not undermine my professional role, interfere with my work duties and will be in accordance with the staff code of conduct policy and the Law.

15. I will not create, transmit, display, publish or forward any material online that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role or the college into disrepute.

16. I will promote online safety with the students in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.

17. If I have any queries or questions regarding safe and professional conduct online either in college or off site, I will discuss them with my line manager or any other member of the Senior Leadership Team.

18. I understand that my use of the college information systems, including any devices provided by the college, including the college internet and college email, may be monitored (e.g. eSafe software) and recorded to ensure the safety of children and staff and to ensure policy compliance. This monitoring will be proportionate and will take place in accordance with data protection, privacy and human rights legislation.

19. I understand that I am responsible for paying the repair/replacement costs for any damage, beyond normal wear and tear, that I cause to any devices or equipment owned or leased by the college. I also agree to pay for the replacement of any college-owned or leased devices that are lost or stolen that I have taken off-site.

20. I understand that the college may exercise its right to monitor the use of information systems, including internet access and the interception of emails, to monitor policy compliance. Where it believes unauthorised and/or inappropriate use, or unacceptable or inappropriate behaviour may be taking place, the college may invoke its disciplinary procedures. If the college suspects criminal offences have occurred, the matter will be brought to the attention of the relevant law enforcement organisation.

Failure to follow this policy

I understand that failure to adhere to the terms of this policy will be dealt with under the relevant college disciplinary procedures.

Related WSFC Policies and Procedures

- eSafety (Staff) Policy and Procedure
- Safeguarding (including Child Protection) Policy
- Staff Code of Conduct Policy
- Staff Protection from Harassment and Bullying Policy
- GDPR Policy