ASKHAM BRYAN COLLEGE

Acceptable Use of Information and Communications Technologies RE12

Equality Impact Assessment: Askham Bryan College recognises the importance of the Equality Act 2010 and its duties under the Act. This document has been assessed to ensure that it does not adversely affect staff, students or stakeholders on the grounds of any protected characteristics.

1. POLICY STATEMENT

1.1 Askham Bryan College is committed to providing a safe and secure environment for all users of its computer networks and communications systems, including all devices connected to those networks and systems.

1.2 Askham Bryan College is committed to providing systems to staff and students to enable them complete their duties/studies effectively. Access to these systems has to be balanced with the need to safe guard these system from misuse or malicious attacks. The main principles of this use is:

- The operation of the ICT Systems relies heavily on the proper conduct of the users, who must adhere to this policy;
- The use of all ICT Systems must be made in compliance with all appropriate legislation e.g. GDPR, Computer Misuse Act, etc;
- The use of all ICT Systems must be made in compliance with all College policies.

2. SCOPE AND LIMITATIONS

2.1 The Acceptable Use of Information and Communications Technologies form part of the conditions of employment, which all employees are required to observe.

2.2 This policy applies to all aspects of the use of Information and Communications Technology (ICT) within the College and usage of systems and services provided by the College from remote locations. This includes but is not limited to;

a) College owned equipment, including:

- Desktop PC's
- Servers
- Laptop/Tablet devices
- Telephones, both fixed and mobile
- Mobile phones

- Digital video camera or camcorders
- Digital audio recording devices
- Reproduction devices (scanners, printers, etc.)
- Any and all software and ICT services provided by the College

b) Privately owned ICT equipment (including personal mobile phones), when:

- Connected to any College owned network
- Utilised to access College software and services
- Made use of on campus, or in the pursuit of College business.

2.3 It is not possible for the College to inspect or audit the content of privately owned devices. Electronic communications from privately owned devices when connected to, or communicating with, the College network will be monitored.

2.4 The same expectations of user behaviour exist when using privately owned devices in the contexts listed above as would exist when using College owned devices. For example, it would not be acceptable to use a privately owned laptop to display obscene images on campus, nor would it be acceptable to use a private mobile phone to send abusive messages on campus.

2.5 This policy applies to all, employees, learners, and any other person permitted to use Askham Bryan College ICT Systems.

3. RESPONSIBILITIES

3.1 Everyone has a responsibility to give full and active support for the policy by ensuring:

- The policy is known, understood and implemented.
- Everyone is treated with respect and dignity.
- Behaviour not in accord with the policy is challenged.

4. CONSEQUENCES OF FALURE TO COMPLY WITH LEGISLATION AND POLICIES

4.1 If a user fails to comply with any legislation or policy, including any of the acceptable use provisions outlined in this document, use of the system may be withdrawn and future access may be restricted. This may impact on the individual's ability to undertake the duties of their job or continue their studies.

4.2 Serious or consistent non-compliance with this policy may be considered to be a disciplinary offence and will be dealt with in accordance with the College's Disciplinary procedure or other appropriate action may be considered.

5. ACCEPTABLE USE

5.1 The following criteria will be used to assess whether usage is acceptable:

- Usage is consistent with College policies and is undertaken by:
- A learner currently enrolled on a course in the support of their studies
- An employee in support of their approved duties
- A contractor in support of work for which they have a current contract with the College.
- An official visitor to the College in support of the purposes of their visit
- Usage is consistent with the regulations appropriate to any external or internal system or network being accessed, i.e. the JaNET Acceptable Use Policy
- Usage of the ICT Systems may be made for limited and reasonable personal usage, provided this is:

  - not associated with monetary reward
  - undertaken in the users own time
  - not interfering with the delivery of College services
  - does not prevent other users from carrying out their studies or assigned duties
  - does not violate this or any other College policy
  - a lawful activity.

- Telephony – The College ordinarily does not allow personal use, with the exception of that outlined in the Mobile Phone Policy.

6. UNACCEPTABLE USE

6.1 It is unacceptable for a user to use, submit, publish, display, download or transmit on or from the ICT Systems, or from privately owned devices used on campus, information which knowingly:

- Restricts or inhibits other users from using the system or the efficiency of the computer systems. Specifically no software, executable files or other potentially harmful material should be downloaded or otherwise installed on the College's systems without the express permission of the Head of IT.
- Violates or infringes on the rights of any other person, including the right to privacy.
- Is contrary to the College's Harassment Policy and Procedures.

- Is in violation of any other College policy.
- Contains defamatory, false, inaccurate, abusive, pornographic, profane, sexually explicit, threatening, racially offensive, or otherwise discriminatory, or illegal material, or personal/private information about any other College employee.
- Encourages the use of controlled substances.
- Uses the system for any other criminal or unlawful purpose, including obtaining unauthorised access to or otherwise interfering with any computer system by 'hacking'.

6.2 It is unacceptable for a user to use ICT systems to:

- Conduct any non-approved business
- Transmit material information, or software in violation of any local or national law;
- Harass an individual or group of individuals
- Make copies of published materials or software when doing so will break copyright laws
- Conduct unauthorised political activity for personal gain or to promote extremist groups or policies
- Conduct any non-College related fund raising or non-College related public relations activities
- Falsify documents or forge a message to make it appear as if it came from another person
- Access or transmit information via the Internet, including e-mail, in an attempt to impersonate another individual
- Conduct any other unauthorised activity (such as sending or forwarding jokes, chain emails and similar material)
- Reproduce any software installed on College's systems without specific authorisation.
- Commit fraudulent activity.
- Transmit images or videos of an individual, or group of individuals, unless it is reasonably believed that consent of the subjects has been obtained.
- Attempt to subvert the course of an ongoing disciplinary procedure.
- Deliberately infect, or attempt to infect, the College systems with a virus or other form

of malware.

- Attempt to monitor traffic on the College network or attempt to connect an unauthorised device with the intention of monitoring traffic.

Clarification of any of the above should be sought from the Head of IT.

7. SECURITY

7.1 Access and usage of systems must be in accordance with the College's Data Security Policy.

7.2 In terms of acceptable usage a user must:

- Not deliberately reveal the account password or allow another person to use their account
- Not use another individual's account
- Not attempt to log on as another user
- Notify the ICT Helpdesk immediately if they identify a security problem, including out of date virus protection.
- Not show or identify a security problem to anyone other than the College's ICT staff or their line manager
- Take reasonable precautions to protect the College's systems from security issues such as computer viruses, spyware and other malware.
- Use only properly supplied and authorised systems for undertaking College business
- Not attempt to circumvent any security measures or virus protection put in place by ICT Services.

8. ETIQUETTE

8.1 When using ICT Systems users must:

- Be polite
- Not use offensive language
- Use caution when revealing their address or phone number (or those of others)
- Be aware e-mail is not guaranteed to be private
- Not intentionally disrupt the network or other users
- Abide by generally accepted rules of network etiquette: for example:

  - Consider who the appropriate recipients of an email should be
  - Do not send emails to a large number of recipients unless it is necessary to do so
  - Consider whether large files or attachments need to be sent, since these will affect system performance.

9. INTERNET

9.1 Access to the internet is provided from all devices connected to the ICT systems. The College reserves the right to withdraw access to the internet from any device, or individual, at the discretion of the Head of IT. Access to and usage of the internet must be in accordance with this policy.

9.2 Use of the internet for personal purposes is permissible provided this usage is in line with the general guidelines for acceptable usage.

10. FILTERING AND ACCESS TO INAPPROPRIATE MATERIAL

10.1 Access to the Internet via the ICT systems is "filtered" to prevent access to certain sites, for example, those containing pornography. The system, however, is not failsafe and the College cannot prevent the possibility that some users may access material that is not consistent with the policies of the College, or in line with the employee's normal duties and responsibilities.

10.2 Where material, which is not consistent with the policies of the College, is inadvertently accessed, people are strongly advised in their own interest to report the matter to their line manager. If there is any doubt as to what constitutes inappropriate material, the user should seek advice from the line manager or ICT Services.

10.3 If a user continues to deliberately access inappropriate material this will be treated as unacceptable use.

10.4 The system must not be used to send or receive illegal material.

11. MONITORING OF INTERNET ACCESS

11.1 Internet access will be regularly and actively monitored by the College to ensure usage is in accordance with this policy. Reports can be provided to Human Resources identifying any staff who have attempted to access material considered inappropriate, illegal or not in compliance with this policy.

11.2 A record of the websites visited by users of the ICT Systems will be maintained for a period in line with GDPR. Access to these logs will be restricted to authorised personnel and will be used for the purposes of diagnosing problems, managing system performance and determining if usage is in accordance with this policy.

12. EMAIL

12.1 Access to internal and external e-mail, is provided on all devices connected to the ICT Systems. The College reserves the right to withdraw access to internal or external e-mail from any device, or individual, at the discretion of the Head of IT.

12.2 Access to and usage of e-mail must be in accordance with this policy and RE19 E-mail policy.

12.3 Use of e-mail for personal purposes is permissible provided this usage is in line with the general guidelines for acceptable usage.

Legal Commitments and E-Mail

12.4 E-mail can result in binding contracts. Users should be aware that legal commitments can result from their e-mails, and the same degree of care should be exercised as with any other written communication.

12.5 For evidential purposes, it is the responsibility of the individual who sends, or receives, the e-mail that a suitable record of any messages which evidence commitments is made in line with GDPR guidelines.

12.6 Personal e-mail accounts, for example, Hotmail, Yahoo, Google mail etc. should not normally be used for official communications.

Dissemination of Information

12.7 When disseminating views or opinions via the College's systems on subjects not directly related to their responsibilities in the College, users will ensure that any opinions or views expressed are not attributed to the College by inserting a suitable disclaimer, for example, "The opinions expressed herein are my own and do not necessarily reflect those of the College".

Monitoring and Logging of E-Mail

12.8 E-Mail access will be regularly and actively monitored by the College to ensure usage is in accordance with this policy.

12.9 In particular monitoring will be undertaken to identify and eliminate any messages which may be harmful to the operation of ICT Systems. For example; e-mails containing viruses, malware, spyware, spam and Phishing e-mails.

12.10 The College reserves the right to maintain records of all e-mail. Records may also be maintained for evidentiary purposes to satisfy funding body or legislative requirements.

12.11 It is not permissible to create an auto forwarding rules in outlook to automatically forward received emails to an external email address. Any attempt to do this will be logged by the system and reported to IT. The person responsible for creating these rules in violation of this policy may face disciplinary action

13. BACK UPS

13.1 ICT Services will take all reasonable measures to ensure that network servers and resources are backed up on a regular basis in accordance with the Backup Policy.

13.2 The ICT department strongly advises users not to store any documents on the local hard drives (i.e. C) of their workstations. It is the responsibility of the user to ensure that any files stored on local hard drives are backed up; furthermore the ICT department must be made aware, in writing, of any machines which have documents stored on their local hard drives.

14. REMOTE ACCESS

14.1 Access to and usage of software or services provided by the ICT Systems from remote locations must be in accordance with this policy and RE14 Portable Equipment and Home Working policy. This includes staff or learners accessing systems from home or from a place of employment.

15. SOCIAL NETWORKING SERVICES

15.1 The use of social networking sites and services is a routine part of everyday life for many users of the internet. Research has found that social networking now surpasses e-mail as the most common internet communications tool. In this environment, it is inevitable that many staff and learners will have digital identities with one or more social networking services.

15.2 Social networking services offer a wide range of tools that can be used to provide learning opportunities and help to engage with learners outside of the classroom. However staff who work in an education establishment have a professional image to uphold and how they conduct themselves online impacts on this image.

15.3 Social networks are built around the concept of being able to add other users of the network as a ‘friend’, building a community of likeminded individuals. When learners gain access into a lecturer’s network of friends and acquaintances the dynamic of the relationship is altered. Adding learners as ‘friends’ provides more information than one should share in an educational setting. It is important to maintain a professional relationship with learners.

15.4 When using social networking services it is considered unacceptable for staff to:

- Accept learners as friends on personal social networking sites, any learner-initiated friend requests should be declined
- Initiate friendships with learners.
- Post commentary that could be deemed to be defamatory, obscene, proprietary, or libelous.
- Discuss students or co-workers or publicly criticise College polices or personnel
- Post images that include student on social networking sites

- List their College e-mail address "@askham-bryan.ac.uk" as a contact address for personal social network accounts.

15.5 If you wish to use social network services and sites with your learners you should maintain a separate account for that purpose. Your College e-mail address should be used as the contact address for this account. This account should not be linked or "friended" with any personal accounts you may have. Post only what you want the world to see – it can be extremely difficult to remove something that you have posted.

15.6 Staff and learners should not create pages, sections, news groups or equivalent on social networking services that claim to be linked to or represent the College without authorisation from the Head of Marketing.

15.7 All staff are advised to review the security and privacy settings on all social networking services they use. We recommend that all privacy settings be set to "only friends". "Friends of Friends" will allow anyone who is a friend of any of your friends to see your profile, photos of you, comments you have posted etc.

15.8 Access to and usage of social networking sites must be in accordance with this policy and RE16 E-Safety Policy.

16. MONITORING USAGE AND ACCESS TO SYSTEMS

16.1 All communications and stored information sent, received, created or contained within the College's ICT Systems are the property of the College. The College reserves the right to monitor, log and access all computer, telephone and network activity including internet access and e-mail, with or without notice, to or from any device owned by the College, or connected to the College's ICT Systems.

16.2 Monitoring and access will take place in order to:

- Establish the existence of facts
- To investigate disciplinary issues
- To detect and/or prevent crime
- To ensure that any use (including any personal use permitted by this policy) is lawful and complies with this policy
- To intercept email for operational purposes, such as protection against viruses and forwarding email to the correct destinations.

16.3 The College may make and keep copies of email and other data stored or transmitted on its systems for any of the above purposes. Users should therefore have no expectations of privacy in the use of these systems.

16.4 When recording telephone conversations the College will make every effort to inform

both parties that recording is taking place. This does not apply to the routing monitoring of telephone activity logs which do not contain recordings of conversations.

16.5 Monitoring of usage and access to systems will be made with the authorisation of the Head of IT or their appointed deputy.

17. PREVENT DUTY

17.1 Prevent is one of the four elements of CONTEST, the government's counter-terrorism strategy. It aims to stop people becoming terrorists or supporting terrorism.

17.2 The Prevent strategy:

- responds to the ideological challenge we face from terrorism and aspects of extremism, and the threat we face from those who promote these views
- provides practical help to prevent people from being drawn into terrorism and ensure they are given appropriate advice and support
- works with a wide range of sectors (including education, criminal justice, faith, charities, online and health) where there are risks of radicalisation that we need to deal with
- The strategy covers all forms of terrorism, including far right extremism and some aspects of non-violent extremism.
  The government defines extremism as "vocal or active opposition to fundamental British values, including democracy, the rule of law, individual liberty and mutual respect and tolerance of different faiths and beliefs". The aim of the Prevent Duty, as set out in the Counter-Terrorism Bill 2015 and incumbent on us as a Further Education College to meet, is as follows;
- 'To stop individuals being drawn into terrorism. This includes violent and nonviolent extremism which in turn can create an atmosphere conducive to terrorism and can popularise views which terrorism may seek to exploit.'
- Our policies as a College are written so as to incorporate the Prevent Duty, where appropriate.

17.3 We shall endeavour through all of our IT policies to ensure that both staff and students of the College are protected under the Duty from accessing or being exposed to material of extremist nature, by effective use of web filters when accessing the internet using College systems and Wi-Fi. We will also encourage staff and students to be aware of e-safety issues through online and in–class tutorial sessions. The Head of IT will also undertake regular audits of our firewall and security provision to ensure it is fit for purpose within the Duty.

18. MONITORING AND REVIEW

18.1 The Head of IT will maintain oversight of the effectiveness of these arrangements. This

policy and the implementation arrangements which underpin it will be reviewed bi-annually by the Head of IT.

19. SUPPORTING/RELATED DOCUMENTS

- Portable Equipment & Home Working Policy (RE14)
- Data Protection Policy (GA23)
- Information Security Policy (RE15)
- E-Policy (RE16)
- Control of IT Hardware and Software (RE18)
- Email Policy (RE19)
- Social Media Communication Policy (QA14)

20. REGULATIONS

20.1 In all aspects of computer usage the College will comply with the following legislation:

- GDPR 2018
- Computer Misuse Act 1990
- Freedom of Information Act 2000
- Copyright Designs & Patents Act 1988
- Malicious Communication Act 1988
- Criminal Justice & Public Order Act 1994