CARFAX
COLLEGE

ACCEPTABLE USE OF TECHNOLOGY POLICY FOR STUDENTS

This policy is addressed to all students, and parents/carers are encouraged to read it with their child. A copy of the policy is available to parents on request and Carfax College actively promotes the participation of parents/carers to help the College safeguard the welfare of students and promote the safe use of technology.

This policy relates to all technology, computing and communications devices, network hardware and software and services and applications associated with them including:

- the internet
- email
- mobile phones and smartphones
- desktops, laptops, netbooks, tablets/phablets
- personal music players
- devices with the capability for recording and/or storing still or moving images
- social networking, micro blogging and other interactive web sites
- instant messaging (including image and video messaging via apps such as Snapchat and WhatsApp), chat rooms, blogs and message boards
- webcams, video hosting sites (such as YouTube)
- gaming sites
- Virtual Learning Environments such as Firefly

This policy applies to the use of technology on college premises.

This policy also applies to the use of technology off school premises if the use involves students or any member of the college community, or where the culture or reputation of the college are put at risk.

Internet

The college provides internet access to students to support their academic progress and development.

For the protection of all students, their use of the internet will be monitored by the college. Students should remember that even when something that has been downloaded has been deleted, it can still be traced on the system. Students should not assume that files stored on servers or storage media are always private.

CARFAX
COLLEGE

Procedures

Students are responsible for their actions, conduct and behaviour when using technology at all times. Use of technology should be safe, responsible, respectful to others and legal. If a student is aware of misuse by other students s/he should report it to a teacher as soon as possible.

Any misuse of technology by students will be dealt with under the college's Behaviour Policy.

Students must not use their own or the college's technology to bully others. Bullying incidents involving the use of technology will be dealt with under the college's Anti-Bullying Policy. If a student thinks that s/he might have been bullied or that another person is being bullied, s/he should talk to a tutor or other member of staff about it as soon as possible. (See also the college's Anti-Bullying Policy).

If a student is worried about something that s/he has seen on the internet, or on any electronic device, including on another person's electronic device, s/he must tell a tutor or other member of staff about it as soon as possible.

In a case where the student is considered to be vulnerable to radicalisation they may be referred to the Channel programme. Channel is a programme which focuses on support at an early stage to people who are identified as being vulnerable to being drawn into terrorism.

In addition to following the procedures in the relevant policies as set out above, all serious incidents involving technology must be reported to the Designated Safeguarding Lead and the IT Manager who will record the matter centrally in the Technology Incidents Log.

Sanctions

Where a student breaches any of the college rules, practices or procedures set out in this policy or the appendices, the Proprietorial Body of Carfax College have authorised the Principal to apply any sanction which is appropriate and proportionate to the breach in accordance with the college's Behaviour Policy including, in the most serious cases, expulsion. Other sanctions might include: increased monitoring procedures, withdrawal of the right to access the college internet facilities and/or detention. Any action taken will depend on the seriousness of the offence.

Unacceptable use of electronic devices or the discovery of inappropriate data or files could lead to confiscation of the device or deletion of the material in accordance with the practices and procedures in this policy and the college's Behaviour Policy

The college reserves the right to charge a student or his / her parents for any costs incurred to the college as a result of a breach of this policy.

CARFAX COLLEGE

APPENDIX 1

Access and Security

Access to the internet from the college's devices and network must be for educational purposes only. You must not use the college's facilities or network for personal, social or non-educational use outside the permitted times specified by the School / without the express, prior consent of a member of staff.

You must not knowingly obtain (or attempt to obtain) unauthorised access to any part of the college's or any other computer system, or any information contained on such a system.

No laptop or other mobile electronic device may be connected to the School network without the consent in writing of the IT Manager who in turn will check that appropriate anti-virus software is installed on the device.

Passwords protect the college's network and computer system. You must not let anyone else know your password. If you believe that someone knows your password you must change it immediately.

You must not attempt to gain unauthorised access to anyone else's computer or to confidential information to which you are not authorised to access. If there is a problem with your passwords, you should speak to your tutor or contact the ICT support.

You must not attempt to access or share information about others without the permission of a member of staff. To do so may breach data protection legislation and laws relating to confidentiality.

The college has a firewall in place to ensure the safety and security of the college's networks. You must not attempt to disable, defeat or circumvent any of the School's security facilities. Any problems with the firewall must be reported to your tutor or IT Manager.

The college has filtering systems in place to block access to unsuitable material, wherever possible, to protect the welfare and safety of students. You must not try to bypass this filter.

Viruses can cause serious harm to the security of the college's network and that of others. Viruses are often spread through internet downloads or circulated as attachments to emails. If you think or suspect that an attachment, or other downloadable material, might contain a virus, you must speak to IT Manager before opening the attachment or downloading the material.

You must not disable or uninstall any anti-virus software on the college's computers.

The use of location services represents a risk to the personal safety of students and to college security. The use of any website or application, whether on a college or personal device, with the capability of identifying the user's location while you are on college premises or otherwise in the care of the college is strictly prohibited at all times.

You must not attempt to add applications to the any college devices without the express consent of the IT Manager and the Head of ICT & Computing.

Methods for overcoming limitations placed on a school device such as 'jailbreaking' are treated with the upmost seriousness.

Use of internet and email

The college does endeavour to provide continuous internet access. Email and website addresses at the college may change from time to time.

Use of the internet

You must use the college computer system for educational purposes only and are not permitted to access interactive or networking web sites outside the permitted times specified by the college without the express prior consent of a member of staff.

You must take care to protect personal and confidential information about yourself and others when using the internet, even if information is obtained inadvertently. You should not put personal information about yourself, for example your full name, address, date of birth or mobile number, online.

You must not load material from any external storage device brought in from outside the college onto the college's systems, unless this has been authorised by the IT Manager.

You should assume that all material on the internet is protected by copyright and such material must be treated appropriately and in accordance with the owner's rights – you must not copy (plagiarise) another's work.

You must not view, retrieve, download or share any offensive material. Offensive material includes, but is not limited to, content that is abusive, racist, considered to be of an extreme or terrorist related nature, sexist, homophobic, any form of bullying, pornographic, defamatory or criminal activity. Use of technology in this way is a serious breach of discipline and may constitute a serious criminal offence. You must tell a member of staff immediately if you have accidentally read, downloaded or have been sent any offensive material or material that is inappropriate, including personal information about someone else.

You must not communicate with staff using social networking sites or other internet or web based communication channels unless this is expressly permitted for educational reasons.

You must not bring the college into disrepute through your use of the internet.

CARFAX
COLLEGE

Use of email

You must not use any personal web-based email accounts such as Gmail, Yahoo or Hotmail through the college's network outside the permitted times specified by the college without the express, prior consent of a member of staff.

You must not read anyone else's emails without their consent.

Use of mobile devices

"Mobile electronic device" includes but is not limited to mobile phones, smartphones, smart watches, tablets, laptops and MP3/MP4 players.

All mobile electronic devices brought onto college premises are not permitted to be registered on the college's Wi-Fi network.

Students are not permitted to use their mobile phones or smartphones (including the use of smart watches) in lessons unless their tutor has given permission for them to do so.

All devices are brought into college at the student's own risk. All devices should require a pass code or password to be unlocked and this should never be divulged to any other student. Please be aware that the school insurance does not cover the loss of mobile phones.

You must not bring mobile electronic devices into examination rooms under any circumstances, except where special arrangements for the use of a tablet or laptop have been agreed with the Principal in writing.

You must not communicate with staff using a mobile phone (or other mobile electronic device), except when this is expressly permitted by a member of staff, for example when necessary during an educational visit. Any such permitted communications should be brief and courteous.

Use of electronic devices of any kind to bully, harass, intimidate or attempt to radicalize others will not be tolerated and will constitute a serious breach of discipline, whether or not you are in the care of the college at the time of such use. Appropriate disciplinary action will be taken where the college becomes aware of such use (see the college's Anti Bullying Policy and Behaviour Policy) and the college's safeguarding procedures will be followed in appropriate circumstances (see the college's Safeguarding and Child Protection Policy and Procedures).

Mobile electronic devices may be confiscated and searched in appropriate circumstances. You may also be prevented from bringing a mobile electronic device into the college temporarily or permanently and at the sole discretion of the Principal.

The college does not accept any responsibility for the theft, loss of, or damage to, mobile electronic devices brought onto college premises, including devices that have been confiscated or which have been handed in to staff.

CARFAX COLLEGE

Photographs and images

Using photographic material of any kind to bully, harass or intimidate others will not be tolerated and will constitute a serious breach of discipline.

No photograph or video should be taken of any other student or staff member without their express permission.

You may only use cameras or any mobile electronic device to take a still or moving image with the express permission of the member of staff in charge and with the permission of those appearing in the image.

You must allow staff access to images stored on mobile phones, cameras or devices and must delete images if requested to do so.

The posting of images which in the reasonable opinion of the Principal is considered to be offensive or which brings the school into disrepute on any form of social media or websites such as YouTube etc. is a serious breach of discipline and will be subject to disciplinary procedures whatever the source of the material, irrespective of whether the image was posted using School or personal facilities.

Sexting

'Sexting' means the taking and sending or posting of images or videos of a sexual or indecent nature, usually through mobile picture messages or webcams over the internet.

Sexting is strictly prohibited, whether or not you are in the care of the School at the time the image is recorded and / or shared.

Sexting may also be a criminal offence, even if the picture is taken and shared with the permission of the person in the image.

Remember that once a photograph or message is sent, you have no control about how it is passed on. You may delete the image but it could have been saved or copied and may be shared by others.

Images shared online become public and may never be completely removed. They could be found in the future by anyone, even by universities and future employers.

The School will treat incidences of sexting (both sending and receiving) as a breach of discipline and also as a safeguarding matter under the School's child protection procedures (see the School's Safeguarding and Child Protection Policy).

CARFAX
COLLEGE

If you are concerned about any image you have received, sent or forwarded or otherwise seen, speak to any member of staff for advice.

Safe use of technology

Carfax College wants students to enjoy using technology and to become skilled users of online resources and media. It recognises that this is crucial for further education and careers.

The college will support students to develop their skills and make internet access as unrestricted as possible, whilst balancing the safety and welfare of students and the security of our systems. Students are educated about the importance of safe and responsible use of technology to help them to protect themselves and others online.

Students may find the following resources helpful in keeping themselves safe online:

http://www.thinkuknow.co.uk/

http://www.childnet.com/

http://www.childline.org.uk/Pages/Home.aspx

http://www.ceop.police.uk

Remember **SAFEBOOK:**

- **THINK** before you post a message or image
- Only connect with **FRIENDS**
- Be **KIND** to others
- Don't share your **PASSWORD**
- Keep your settings **PRIVATE**
- Don't be **HURTFUL** to others

If you are unhappy with something that you receive via social media, the internet or email…

TELL, UNFRIEND, BLOCK, REPORT

CARFAX
COLLEGE

Student User Agreement for the Student Acceptable Use Policy

I agree to follow the college rules on the use of the school network resources. I agree to report any misuse of the network to a member of SLT.

If I do not follow the rules, I understand that this may result in loss of access to these resources as well as other disciplinary action. I realise that students under reasonable suspicion of misuse in terms of time or content may have their usage monitored or their past use investigated.

Student Name: _____

Student Signature: _____

Parent/Carer's/Guardian's Name: _____

Parent/Carer's/Guardian's Signature: _____

Date: __/__ /_____