It is intended that this policy is 'fair to all'. Where any part could potentially lead to unequal outcomes, the policy then justifies why this is a proportionate means of achieving a legitimate aim.

SWINDON COLLEGE: POLICIES AND PROCEDURES

Title:	**Student Online safety & Acceptable Use Policy**
Owner:	**DRF**
Date:	**June 2018**
Review Date:	**June 2019**

Scope - This procedure deals with the protection of all students at Swindon College when using ICT resources, and articulates what is deemed to be acceptable and unacceptable use of said ICT resources. Whilst we aim to support the full use of the vast educational potential of new technologies we also have a responsibility to provide safeguards against risk, unacceptable material and activities. These guidelines are designed to protect all users from on-line safety incidents and promote a safe e-learning environment for students.

The College believes that all students should be trusted and enabled to use digital technologies in a principled and productive way. All students should be given the opportunity to make productive decisions in the ways they decide to use digital technologies and should be fully engaged in the on-going debate about what responsible digital citizenship means and how we can nurture it within our College.

The breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk:

- **content**: being exposed to illegal, inappropriate or harmful material; for example pornography, fake news, racist or radical and extremist views;
- **contact:** being subjected to harmful online interaction with other users; for example commercial advertising as well as adults posing as children or young adults; and
- **conduct**: personal online behaviour that increases the likelihood of, or causes, harm; for example making, sending and receiving explicit images, or online bullying.

Education — Students

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in on-line safety is therefore an essential part of the College's on-line safety provision. Students need the help and support of the College to recognise and avoid on-line safety risks and to build their resilience.

On-line safety education will be provided in the following ways:

- A planned on-line safety programme should be provided as part the Tutorial system.
- Students should be taught to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information on all relevant teaching programmes.
- Students should be helped to understand and adopt safe and appropriate use of IT, the internet and mobile devices both within and outside College.

- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Through staff acting as good role models in their use of ICT, the internet and mobile devices.
- On-line safety should be a focus in all areas of the curriculum and staff should reinforce on-line safety messages in the use of ICT across the curriculum.
- Where students are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that IT Services Staff can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.
- The safe use of IT must be reinforced and supported in terms of ensuring appropriate and adequate measures are in place to mitigate the risk posed by extremist material and on-line radicalisation in line with Prevent Duty guidance.

Whilst it iis recognised that mobile communications technology (i-pads, tablets, I-phones, Androids etc.) can be of tremendous benefit to students within the teaching and learning environment it is also recognised that the unlimited and unrestricted usage of 3G and 4G internet access can pose a risk to the safety of students. The College will not seek to block access to the internet by these means but we do commit to a consistent teaching and awareness approach with students of the dangers presented by the internet and how they can be mitigated.

The College will continue to utilise the 360 degree safety self review tool to monitor and develop our approaches to E-safety.

Education — Parents/Carers

Many parents and carers have only a limited understanding of on-line safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of their sons' and daughters' on-line experiences. The College will therefore seek to provide information and awareness to parents and carers through the College website and awareness sessions offered at parents' evenings

Education & Training — Staff

It is essential that all staff receive on-line safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal on-line safety training will be made available to staff.
- All new staff should receive on-line safety training as part of their safeguarding training.

Training — Governors

The College Link Governor will receive on-line safety briefings through the College Safeguarding Steering Group.

Acceptable Use of ICT
Examples of acceptable use are:

- Using web browsers to obtain information from the Internet
- Accessing databases for information as needed.
- Using e-mail for contacts.
- Using the college's network to promote the exchange of information to further education and research and is consistent with the mission of the college.
- Using the network and Internet in a manner, which respects the rights and property of others.

- Keeping all accounts and passwords confidential and inaccessible to others.
- Showing responsibility by making backup copies of material critical to you.
- Showing responsibility by taking precautions to prevent viruses on the college's equipment.
- Upon receipt of an attachment checking to making sure it is from a known source.
- Backing out of an accidentally encountered site that contains materials that violate the rules of acceptable use, and notifying a member of staff of the occurrence immediately.
- Logging out or locking computers when they are left unattended
- Recognising that electronic communications sent through or stored on the college's network will be treated as college related and may be monitored or examined by authorised delegates on a case by case basis for operational, maintenance, compliance, auditing, security and/or investigative purposes
- Reporting any damage to or loss of computer hardware immediately
- Saving documents onto appropriate storage areas of the college network or other appropriate storage systems
- Reporting any inappropriate behaviour and online bullying to the Safeguarding Team
- Taking reasonable care that there is no damage or loss of any equipment on loan from college

Examples of unacceptable use are:

- Use of the Internet for purposes that are illegal, unethical, harmful to the college, or nonproductive.
- Sending or forwarding chain e-mail, i.e., messages containing instructions to forward the message to others.
- Recording, filming or take photographs on college premises without permission.
- Broadcasting e-mail, i.e., sending the same message to more than 10 recipients or more than one distribution list.
- Relocating college information and communication equipment without prior permission
- Conducting a personal business using college resources.
- Transmitting any content that is offensive, harassing, likely to promote and foment extremist/radical views, or is fraudulent.
- Using inappropriate language: do not swear, use vulgarities or sexual innuendos.
- The sending of material likely to be offensive or objectionable to recipients.
- Using programs that harass college users or infiltrate a computing system and/or damage the software components is prohibited.
- Changing original software setting/configuration of college owned computers
- Doing harm to other people or their work.
- The unauthorised installation of software on college computers without clearance from the IT Team.
- Doing damage to the computer or the network in any way.
- Interfering with the operation of the network by installing illegal software, shareware, or freeware.
- Plagiarisation and violation of copyright laws.
- Conversation in email using all upper case letters. This is considered shouting.
- Sharing your passwords with another person. Doing so could compromise the security of your files.
- Wasting limited resources such as disk space or printing capacity.
- Trespassing in another's folders, work, or files.
- Removing software CDs from their rightful location
- Giving out personal information such as your home address or telephone number. Use the college's address instead, but not the college's phone number.
- Downloading material from the Internet without specific authorisation from the IT manager.
- Viewing, sending, or displaying offensive messages or pictures.
- Accessing sites that contain pornography; that spread hatred; that promote discrimination; that give instruction for acts of terrorism, harassment, murder, suicide, or other illegal activity.

Use of digital and video images – Photographic, Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff and students need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. The College will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm.

When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

Staff are allowed to take digital/video images to support educational aims, but must follow College policies concerning the sharing, distribution and publication of those images, where parental/student permission is given (on parental consent forms). Care should be taken when taking digital/video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the College into disrepute.

Students must not take, use, share, publish or distribute images of others without their permission.

Photographs published on the College website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images. Students' full names will not be used anywhere on a website or blog, particularly in association with photographs. Written permission from parents or carers will be obtained before photographs of students are published on the College website or prospectus. Student's work can only be published with the permission of the student and parents or carers.

Social Media

Whilst valuing the use of social media (Facebook, Twitter etc) as an educational and marketing tool, staff and students need to be aware of the risks associated with its use. Items published on social networks have the potential to remain available forever and may cause harm or embarrassment to individuals or the College in the short or longer term. Publishing negative or untrue items about an individual or organisation can lead to College disciplinary, civil action and/or criminal prosecution.

All instances of cyber-bullying and/or harassment will be investigated thoroughly and addressed through the Anti-Bulling Policy.

'Sexting' is an increasingly common activity among children and young people, where they share inappropriate or explicit images online or through mobile phones. It can also refer to written messages.

'Sexting' is the exchange of self-generated sexually explicit images, through mobile picture messages or webcams over the internet. It may be common but 'sexting' is illegal. By sending an explicit image, a young person is producing and distributing child abuse images and risks being prosecuted, even if the picture is taken and shared with their permission.

When images are stored or shared online they become public. They can be deleted on social media or may only last a few seconds on apps like Snapchat, but images can still be saved or

copied by others. These images may never be completely removed and could be found in the future, for example when applying for jobs or university.

Young people may think 'sexting' is harmless but it can leave them vulnerable to:

- Blackmail - An offender may threaten to share the pictures with the child's family and friends unless the child sends money or more images.
- Bullying - If images are shared with their peers or in school, the child may be bullied.
- Unwanted attention - Images posted online can attract the attention of sex offenders, who know how to search for, collect and modify images.
- Emotional distress – Young people can feel embarrassed and humiliated. If they are very distressed this could lead to suicide or self-harm.

The College will ensure that a supportive and enabling stance is adopted whenever dealing with students affected by any aspect of negative internet usage.

Staff using social media for educational or other College work purposes, are responsible for the monitoring of its content.

Guidance for implementation

Any allegation or incidence of a breach of On-line safety for staff or students must be taken seriously and investigated appropriately. In the first instance the incident or allegation must be recorded and reported to a member of the Safeguarding Team or to the reporting person's immediate line manager.

The allegation or incidence will then be subject to a formal investigation with the findings recorded and subsequent actions taken as appropriate.

June 2018