Internet Online Safety Policy

2020-21

Signature: [Signature]

Headteacher

Approval Date: July 2020

Review Date: July 2021
Internet and Online/E-safety at West Somerset College

Aim:

We recognise the value of modern technology systems and welcome their development. We continually strive to enhance their appropriate use (both within college and outside) in order to promote the educational attainment of our students. This policy is of paramount importance as our students’ access to technology is currently becoming universal and increasingly more mobile. The technologies encompassed by this policy include all computer and internet technologies and electronic communication devices such as mobile phones and PDAs.

Any cases of a breach of the policy will be referred to the SLT member responsible for IT systems.

Introduction

The use of technology has become a significant component of many safeguarding issues. Child sexual exploitation; radicalisation; sexual predation and online bullying: technology often provides the platform that facilitates harm. An effective approach to online safety empowers parents and the college to protect and educate the whole college or college community in their use of technology and establishes mechanisms to prevent, identify, intervene in and escalate any incident where appropriate and where a child is at risk.

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.

Filters and monitoring

West Somerset College will be doing all that they reasonably can to limit student’s exposure to the above risks from the college’s IT system. As part of this process, we will ensure the college has appropriate filters and monitoring systems in place.

In relation to the college’s responsibility towards safeguarding and promoting the welfare of students, we provide them with a safe environment in which to learn, we consider the age range of the students, the number of students, how often they access the IT system and the proportionality of costs versus risks.

Whilst filtering and monitoring are an important part of the online safety picture for our college to consider, it is only one part. We also consider a whole school approach to online safety. This includes a clear policy on the use of mobile technology in the college. Many students have unlimited and unrestricted access to the internet via 3G and 4G in particular and the college does not allow use of these devices at all on our premises between 08.45 and 15.15.

Whilst it is essential that we ensure that appropriate filters and monitoring systems are in place, we will be careful that “over blocking” does not lead to unreasonable restrictions as to what students can be taught with regard to online teaching and safeguarding.
Use of the internet within the college

Amongst the uses of the internet within college are the following:

- Access to learning wherever and whenever convenient.
- Access to world-wide educational resources including museums and art galleries.
- Access to experts in many fields for students and staff.
- Professional development for staff through access to national developments, educational materials and effective curriculum practice.
- Access to GCSE revision sites
- Access to Show My Homework an online homework software package

Student safety on the school internet system

- The school internet facility has been designed expressly for student use and includes filtering appropriate to the age of students.
- Students are taught what internet use is acceptable and what is not and given clear objectives for Internet use.
- Internet access is planned to enrich and extend learning activities.
- Staff guide students in on-line activities that will support learning outcomes and plan for the students’ age and maturity.
- Students are educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Gaining access to the school internet

- The school maintain a current record of all system users (including staff and students) who are granted internet access.
- All students must read and accept the ‘Student ICT Acceptable use policy’ before using any school ICT resource. (Appendix 1)

Inappropriate usage of internet and loss of privilege

Any student in breach of the agreement for usage of the Internet will have their access curtailed immediately pending an investigation.

Social Networking services

Access to Social Networking services (for example Twitter, YouTube, Facebook, Instagram, Snapchat, etc.) is forbidden in school and all such sites are blocked. Students using such sites outside of school have a duty to use them responsibly. Any incident of slander, abuse or defamation perpetrated on a social networking site which impacts upon one of our students, shall be treated as Cyber-bullying and shall be sanctioned in accordance with the school’s behaviour policy.

School website

The contact details on the website are the school address, e-mail and telephone number. Student personal information is not and shall not be published.
Publishing students’ images and work

- Photographs that include students will be selected carefully and will be appropriate for the context.
- Students’ full names will only be used when featured on news articles sent to press.
- No photographs of students are published on the school website without permission from the parent/carer.

Information system security

- School ICT systems’ capacity and security are reviewed regularly.
- Virus protection is updated regularly.
- Security strategies are discussed regularly.

Protecting personal data

Personal data is recorded, processed, transferred and made available according to the Data Protection Act 1998.

Assessing risks

The school takes all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school can accept no liability for the material accessed, or any consequences of Internet access.

Handling e-safety complaints

- Any complaint about student misuse must be referred to the Achievement Leader.
- Complaints of a safeguarding nature must be dealt with in accordance with the school’s safeguarding procedures and should be recorded on My Concern or reported to the Designated Safeguarding Lead.
- Parents can report through our safeguarding email address wscsafeguarding@educ.somerset.gov.uk

Communication of Policy

- Students are informed that internet use will be monitored.
- Students are asked to read and accept the Student ICT Acceptable Use Policy before accessing the network. (Appendix 1)

Information and guidance

We offer all our students a wide variety of ICT resources which are under constant improvement and development. They are offered access to the West Somerset College network, internet and electronic mail (email). Keeping our students ‘safe’ on the internet and supporting them to use the network appropriately is one of our key responsibilities. As a consequence we operate a ‘Student ICT Acceptable Use Policy’ and hope that parents/carers will support us. The ‘Student ICT Acceptable Use Policy’ will be explained to all new students during their first 2 weeks in school and then reiterated annually. Access to the West Somerset College network, internet and electronic mail (email) will stop once students have left the school.
At the outset we must emphasise that the majority of our students use the network, internet and electronic mail (email) safely and sensibly and this document acts to increase awareness for all. We take any infringement of the ‘Student ICT Acceptable Use Policy’ very seriously and have installed software to monitor the use of the network, internet and email. Any case reported will be thoroughly investigated and judged on an individual basis. Students should expect serious sanctions to apply.

It is the college's policy that every reasonable step should be taken to prevent exposure of students to undesirable materials/contacts on the internet, including extremist propaganda or any site promoting radicalisation of any sort. It is recognised that this can happen not only through deliberate searching for such materials, but also unintentionally when a justifiable internet search yields unexpected results. To reduce such occurrences, the college has its own dedicated broadband line and filter. This facility stops students accessing sites deemed inappropriate for use at school and also provides a full audit trail. We believe that the benefits to students from access to the internet exceed any disadvantages.

However, as with any other area, parents/carers are responsible for setting and conveying the standards that their sons/daughters should follow when using media and information sources. The college therefore supports and respects each family’s right to decide whether or not to apply for access. During the college day, teachers will guide students towards appropriate material. At home, families bear the same responsibility for guidance as they exercise with other information sources such as television, telephones, films and radio.

YouTube, Instagram, Snapchat, Facebook, Twitter, Pinterest and Tiktok; these are the names of well-known and popular websites many people - adults and children - will probably have come across. When used positively they allow people to share music, video, art, opinion, collaborate on work or indeed just have social discussions. Most of the content is harmless; other content can be cruel and cutting. The sites are not rigorously censored in terms of content. For example, on YouTube the BBC is putting video trailers for its forthcoming TV programmes whilst other contributors are posting more material that is inappropriate. The other sites allow ‘members’ to write about themselves, and other people of course and not all of it is appropriate.

Anyone can view the content on YouTube, although for access to some sites users have to register details on the site. Access to these sites is very easy. For students, having their own ‘social networking’ space is a very popular thing to have, but both parents/carers and students are not always aware of the risks they face when using sites like Facebook, Instagram or Snapchat. One of the rules that you may not be aware of is the minimum age for the sites such as Facebook is 13. Please see the graphic below for the age restrictions for different social media platforms.
It is worth remembering that these are public spaces and so anyone can view and use the information how they please. Your son/daughter may already be a member of them and a contributor, not just a reader of material. That means they have access to material, which you may well consider inappropriate. The users of these sites have the ability to create their own material and post whatever they like on to their site i.e. films, images or text. As it is accessed solely by user identification and a password, it is their choice who views it and whom they choose to pass it to.

**Here are the main e-safety issues, which should be discussed with your son/daughter:**

- **Personal Identity Fraud:** there is a concern if students post personal details or complete online surveys. They should avoid giving out their full name, mailing address, telephone number, the name of their school, or any other information that could help someone determine their actual identity.

- **Public Domain Information:** all images, comments are stored and made available to the public. There are privacy settings and they should be used.

- **Online Bullying:** this can be in the form of comments, blog entries and chat rooms. Students must not send, share and upload of images, photos or videos that:
  - are illegal, obscene, defamatory;
  - bring the school into disrepute or
  - are intended to annoy or intimidate another person.

- **Exploitation/ Misrepresentation:** clearly people may try to make contact with students and they may not be who they say they are. Students should never meet anyone they have met online.

You know your son/daughter best. Visit the sites and see for yourself what’s being said and the potential of what could be said or shown. Ask your son/daughter if they use the sites at all. If so you might engage in a discussion with them about the issues we have highlighted above. The websites can be useful and are a part of life nowadays. However educating our children on the issues will mean they can use them safely.

Electronic mail (email) provides a quick and effective means of communication. Students must be made aware that they will be held responsible for the content of any email message they transmit and that they should not contain messages using language or content that is unacceptable. It is also recognised that some people may try to use email to identify and contact students for unacceptable reasons.

To avoid these problems the school has adopted the Local Authority’s system for filtering all emails sent or received. The following points should be supported at all times:

Steps should be taken to verify the identity of any school, organisation, adult or child seeking to establish regular email with the school or its students.

Students should avoid revealing their identification within email messages. Students should only be identified by their network username and the student’s own address is never revealed.

Information should never be given that might reveal a student’s identity or their current whereabouts.

We also have a number of websites from national bodies that explain issues further and also cover internet use at home. These can be found on our website as follows:
This document aims to outline the key aspects of using the ICT facilities but if you require any further advice please contact the school.