eSafety Policy

Version No	Purpose/Change	Lead	Impact Assess	Date
Previous versions available				
9.0	Reviewed and updated	BW		February 2023
-	Reviewed – no changes	CAP		January 2024

Introduction

Wilberforce Sixth Form College recognises the benefits and opportunities which new technologies offer to teaching and learning. We encourage the use of technology in order to enhance skills and promote achievement. However, the accessible and global nature of the internet and variety of technologies available mean that we are also aware of potential risks and challenges associated with such use. The term 'eSafety' is used to encompass the safe use of online technologies in order to protect students and staff from known and potential risks. In furtherance of our duty to safeguard students and staff, we will do all that we can to make our students and staff stay eSafe and to satisfy our wider duty of care. This eSafety Policy should be read in conjunction with other relevant College policies: Safeguarding, Child Protection, Staff Code of Conduct, Student Conduct and Behaviour for Learning, Acceptable IT Use, Anti-Bullying and also the eSafety guidance for students.

Policy Scope

The policy applies to all members of the College community who have access to the College IT systems, both on the premises and remotely. Any user of College IT systems must adhere to the eSafety Policy and Acceptable Use Policy. The eSafety Policy applies to all use of the internet and electronic communication devices such as email, Microsoft Teams, mobile phones (inc. 'smart' phones), social networking sites (including on-line gaming), e.g. Facebook, Twitter, etc.

The breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas of risk:

- Content: being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.

- Contact: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
- Conduct: online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and nonconsensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images, harmful online challenges, hoaxes and online bullying.

- Commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams.

It is essential that the college community are aware of these issues and are educated to identify risk and know who to report concerns to and how to remain safe online.

Roles and Responsibilities

There are clear lines of responsibility for safeguarding students within the College and eSafety comes under this. See the Safeguarding and Child Protection Policies on the College website. The first point of contact should be the Student Services Manager (Lead Person for Child Protection) who is located in Student Services. All staff are responsible for ensuring the safety of learners and should report any concerns immediately following the guidance within the Child Protection Policy.

All staff are required to complete annual safeguard training, and to be made aware of the eSafety, child protection, staff code of conduct, the role of the Designated Senior Person for Safeguarding and student behaviour and associated policies. When informed about an eSafety incident, staff members must take particular care not to guarantee any measure of confidentiality towards either the individual reporting it, or to those involved.

All students must know what to do if they have eSafety concerns and who to talk to. In most cases, this will be their Teacher or Academic Mentor who will then report this to the Designated Senior Person for Safeguarding, Lead Person for Child Protection or a Child Protection Officer following the Child Protection guidelines. Where it is considered appropriate, the College will involve additional support from external agencies.

Specific roles and responsibilities:

Designated Senior Person (DSP):

The DSP is responsible for ensuring staff development and training is provided on eSafety, recording incidents, reporting any developments and incidents to the relevant bodies and liaising with the local authority and external agencies to promote eSafety within the College community.

Students:

Students are responsible for using the College IT systems, Microsoft Teams and mobile devices in accordance with the College Acceptable Use Policy, which they agree to during enrolment at the College. Students are expected to seek help and guidance where they are worried or concerned, or where they believe an eSafety incident has taken place involving them or another member of the College community. Students must act safely and responsibly at all times when using the internet and/or mobile technologies.

Students must report any concerns regarding Safeguarding or Child Protection including eSafety issues to Student Services immediately.

Staff:

All staff are responsible for using the College IT systems and mobile devices in accordance with the College Acceptable Use Policy, which they must actively promote through embedded good practice. Staff are responsible for completing training on eSafety and displaying a model example to students at all times.

All digital communications with students must be carried out in a professional manner and contain appropriate content at all times. All staff should apply the relevant College policies (Child Protection and staff code of conduct) and understand the disclosure and concern reporting procedures. Any incident that is reported to or discovered by a staff member must be reported using the guidance set out in the Child Protection Policy. See also the 'Staff Code of Conduct Policy'.

All staff are responsible for considering online safety when planning lessons and schemes of work and should liaise with the DSP if they have any doubt or concerns as to eSafety in these processes.

Security

The College will do all that it can to make sure the College network is safe and secure. Every effort will be made to keep security software up to date. Appropriate security measures include; the use of enhanced filtering, protection, alerts and reports of; firewalls, servers, routers, work stations etc, including the use of the college WIFI to prevent accidental or malicious access of College systems and information, in line with our Prevent, safeguarding and Child protection policies. Digital communications, including email, Microsoft teams and internet postings, over the College network can and will be monitored in line with relevant policies. The college uses Smoothwall web filtering to ensure safe browsing and safeguarding reporting and also Impero for safeguarding reports and classroom control/security patching. All internet use is monitored regularly.

Behaviour

Wilberforce Sixth Form College will ensure that all users of technologies adhere to the standards of behaviour as set out in the Acceptable Use Policy and other relevant policies. The College will not tolerate any abuse of IT systems. Whether offline or online, communications by staff and student should be courteous and respectful at all times. Any reported incident of bullying or other unacceptable conduct will be treated seriously and in line with the student and staff codes of conduct and behaviour policies.

Where conduct is found to be unacceptable, the College will deal with the matter internally. Where conduct is considered illegal, the College will report the matter to the Police or other appropriate agency.

Guidance for staff on the 'Safer Use of Electronic Media' is provided in Appendix 1. Guidance for students will be reinforced during lessons and tutorial sessions. Additional guidance is given to staff and students regarding the appropriate and safe use of remote learning platforms, such as Microsoft teams, within this policy and reinforced throughout the academic year prior to college 'digital days' as appropriate, which are planned remote learning activities.

Use of Mobile Devices

The use of mobile devices and the use of own devices whilst on college site is permitted. To ensure the safety of students and staff whilst using such devices, we insist that any internet use is only permitted by using the college WiFi network. The use of mobile and personal devices within the classroom or learning environment is at the discretion of the member of staff leading the session.

We recognise that child-on-child abuse can take place through the use of personal mobile devices, which creates an opportunity for such abuse to take place on the college premises. It is therefore imperative that students know how to stay safe online, are educated regarding child-on-child abuse issues and know who to report any concerns to.

Personal Information

Any processing of personal information needs to be done in compliance with the Data Protection Act 2018.

Education and Training

With the nature of internet access, it is impossible for the College to eliminate all risks for staff and students. It is our view therefore, that the College should support staff, students and parents/carers through training and education. This will provide them with the skills to be able to identify risks independently and manage them effectively.

For students:

Students will receive guidance on the safe use of IT systems and equipment, including eSafety and staying safe online. Issues associated with eSafety apply across the curriculum and students should receive guidance on what precautions and safeguards are appropriate, when making use of the internet and technologies. Students should also know what to do and who to talk to where they have concerns about inappropriate content, either where that material is directed to them, or where it is discovered as part of a random search. The Acceptable Use Policy is displayed and must be agreed to whenever students log on to the College network. Within classes, students will be encouraged to question the validity and reliability of materials researched, viewed or downloaded. They will also be encouraged to respect the copyright of other parties and to cite references properly.

Students should inform a Child Protection Officer or a member of staff if inappropriate content is accessed or they have any concerns about the access of such material or the conduct or concerns of or about other students.

For staff:

Staff complete Safeguarding and Child Protection training annually and as part of their induction to the College. Further eSafety training is delivered to all staff or groups of staff as appropriate. The Acceptable Use Policy is displayed and must be agreed to whenever staff log on to the College network.

Incidents and Response

Where an eSafety incident is reported to the College, this matter will be dealt with seriously. The College will act immediately to prevent, as far as reasonably possible, any harm or further harm occurring and liaise with any relevant external agencies. If a student wishes to report an incident, they can do so to any member of staff or to Student Services and the Lead Person for Child Protection.

Where a member of staff wishes to report an incident, they must follow the guidance as set out in the Child Protection Policy.

Following any incident, the College will review what has happened and decide on the most appropriate and proportionate course of action. Sanctions may be put in place (in line with the Student Conduct and Behaviour for Learning Policy), external agencies may be involved or the matter may be resolved internally depending on the seriousness of the incident.

Please note: that whilst every effort will be made to follow this policy, circumstances may not always allow this or may render certain parts of the policy inappropriate. Individuals will be treated fairly and in line with legislation in all instances.