

**E-Safety Policy**

City College Limited

69 Steward Street

Birmingham

B18 7AF

|  |  |  |  |
| --- | --- | --- | --- |
| Title | E-Safety Policy | Department | Quality |
| Location | Sharepoint | Author | PWA |
| Approved by SLT | Yes | Date | May 15th 2020 |
| Last Review | January 2021 | Next Review | January 2022 |
| Version | Author | Issue date | Summery |
| V.1 | PWA | May 2020 | First draft |
| V.2 | PWA | January 2021 | Review |

**Key Person(s)**

**Managing Director**

**Associate Director for Quality and Partnerships**

**Higher Education Manager**

**Chief of Staff**

# E-Safety Policy

# Policy Statement

City College recognises e-safety issues and the potential harm and risks it can pose to staff and students. All staff and students have a duty to understand e-safety issues as part of their wider safeguarding duties recognising their role in remaining safe online, free from sexual, emotional, peer to peer and financial abuse. This policy provides a framework for staff and students for following best practice in regard of the definition of e- safety.

The term e-safety is defined for the purposes of this document as the safe and responsible use of technology including the use of the internet and other means of communication using electronic media such as text messages, gaming devices, email and social media otherwise known as Internet and Digital and Mobile Technologies (IDMTs). The promotion of good e-safety is as much about behaviour as it is electronic security, limiting the risks to staff and students when using IDMTs through a combined approach to policies and procedures, infrastructures and education and training.

The City College aim is that all students and staff recognise the risks, dangers and potential harm that may arise from the use of IDMTs. They understand how to mitigate these risks and potential dangers and can recognise, challenge and respond appropriately to any e-safety concerns ensuring other policies and procures such as Safeguarding and Prevent are adhered to.

The following legislation is relevant to this policy.

* + - Health and Safety at Work Act 1974
    - Protection of Children Act 1999
    - Management of Health and Safety at Work Regulations 1999
    - The Human Rights Act 1998
    - Sexual Offences Act 2003
    - The Children Act 2004
    - Safeguarding Vulnerable Groups Act 2006
    - Equality Act 2010
    - Education Act 2011
    - Prevent Duty
    - Protection of Freedoms Act 2012
    - The Counterterrorism and Security Act 2015
    - General Data Protection Regulation 2018
    - Keeping Children Safe in Education 2019

# The College is aware that the understanding and use of IDMT is essential to helping and encouraging every student reach their full potential. The College recognises its duty to raise awareness and educate those involved student welfare and development about the risks of IDMT. Best practice with E-safety is not the removal or banning of access to digital technologies in itself but rather education and training, for staff and students, around responsible use and potential dangers associated with IDMT. This will ensure all staff and students are equipped with the knowledge and skills to safeguard themselves when using IDMT. Training will also ensure staff know how to respond when concerns arise regarding the misuse of IDMT to safeguard those at risk through online activity. All concerns and disclosures regarding safeguarding, including E-Safety should be reported to the Designated Safeguarding Officer (DSO), referring to the Safeguarding and Prevent Policy.

**Roles and Responsibilities**

All staff and volunteers will follow College policy to;

* Advise and educate students as to the safe use of the internet and other technologies through a range of learning strategies.
* Ensure any electronic information, including links and recommendations are safe and age appropriate for students.
* Ensure any students are aware of their legal obligations and that perpetrators who forward indecent images could be prosecuted under s45 of the Sexual Offences Act 2003 for the distribution of child pornography which may result in them being registered on the Sex Offenders Register if convicted.
* Advise students of the risks associated with news groups and the so called ‘fake news’ sites and that some information may be misleading and derogatory.
* Make students aware that they may encounter content on IDMT that distorts and misrepresents what constitutes a good and safe relationship.
* Adhere to the content of this and related policies at all times, demonstrating best practice in the use of IDMT
* Take responsibility for their own network use and not tamper with, disable or circumvent security measures – filters, encryption etc
* Will not have personal information or sensitive electronic data taken offsite without being security encrypted and authorised by management
* Must not introduce unapproved software on to the College network
* Ensure all Email content and tone is professional at all times and never aggressive, derogatory, disparaging or dismissive or in tone which may be hurtful to others. The use of abusive language is expressly forbidden
* Not engage with students through any IDMT not expressly agreed with or managed by the College such as personal emails, social media, chat rooms or online forums or through personal phone lines.
* Not engage with or forward harmful correspondence or chain emails
* Ensure students know how to and are confident to report online abuse or any other Safeguarding issue.
* Ensure all related passwords at least meet the minimum-security requirements, are changed every six months and are never disclosed (see additional guidance below)

In addition to the above, the Senior Leadership Team (SLT) will;

* Will ensure that all IDMT devices have appropriate security and anti-virus protection.
* Ensure the College uses an Internet Service Provider (ISP) who subscribes to the Internet Watch Foundation (IWF) filtering list.
* Ensure IDMT devices are secure and adaptable making internet access and supervision appropriate and suitable for staff, students and the learning environment. Sites should be rejected on the grounds of sexual content, profanity, gambling, violent or other unacceptable content
* Agree where necessary and in advance, for professionals to temporarily access a normally restricted website in order to carry out research for a project or study and the provision this is justified in writing in advance of any access.
* Ensure that regular checks are made to ensure that filtering methods selected are age appropriate, effective and reasonable.
* Provide any and within reason, all IDMT equipment required for staff and students to meet their learning expectations and reach their full potential
* Apply this policy equally and fairly, reporting any abuse in line with other College policies and procedures such as the Bullying and Harassment Policy or the Safeguarding and Prevent Policy

Student use of IDMT is a component part of this policy. All students must;

* Ensure any electronic information, including links and recommendations are safe and contain professional content
* Be aware of their legal obligations and that perpetrators who forward indecent images could be prosecuted under s45 of the Sexual Offences Act 2003 for the distribution of child pornography which may result in them being registered on the Sex Offenders Register if convicted.
* Recognise the risks associated with news groups and the so called ‘fake news’ sites and that some information may be misleading and derogatory.
* Adhere to the content of this and related College policies at all times, demonstrating best practice in the use of IDMT
* Take responsibility for their own network use and not tamper with, disable or circumvent security measures – filters, encryption etc
* Will not have personal information or sensitive electronic data taken offsite without being security encrypted and authorised by a College member of staff
* Must not introduce unapproved software on to the College network or employer networks
* Ensure all Email content and tone is professional at all times and never aggressive, derogatory, disparaging or dismissive or in tone which may be hurtful to others. The use of abusive language is expressly forbidden
* Not engage with College staff through any IDMT not expressly agreed with or managed the College such as personal emails, social media, chat rooms or online forums or through personal phone lines.
* Not engage with or forward harmful correspondence or chain emails
* Report any online abuse or any other Safeguarding issue.
* Ensure all related passwords at least meet the minimum security requirements, are changed every six months and are never disclosed (see additional guidance below)

**Password Protocols**

* All staff and students must always keep their passwords private, must not share with others; If a password is compromised the College should be notified immediately.
* All staff and students have their own unique username and private passwords to access the College systems. Staff are responsible for keeping their password(s) private.
* The College requires staff and students to use STRONG passwords of at least 12 characters containing a combination of at least one capital letter and one number
* Staff and students should change their passwords every six months.
* The College requires staff using critical systems to use two factor authentication.

# Risks associated with IDMT

Students do not always recognise the inherent dangers of the IDMT and often do not understand that online behaviour may have offline consequences. Despite this, digital technologies can offer them opportunities to learn and develop, communicate, be creative and be entertained. The advantages of the internet can and should out-weigh the disadvantages.

Harm in relation to content

* Exposure to age-inappropriate material
* Exposure to inaccurate or misleading information
* Exposure to socially unacceptable material, such as that inciting violence, pornography, hate or intolerance
* Exposure to illegal material, such as images of child abuse.
* Exposure to bullying and harassment
* Risk of impersonation
* Exposure to unwanted sexual advances both image based and not.
* Exposure to self-harm or suicide related content
* Exposure to extremism, radicalisation or terrorist activity
* Threats through harmful programmes and software, virus’, malware and hacking

Harm in relation to contact

* Grooming through the use of communication technologies in an attempt to meet and groom young people or vulnerable adults with the intention of sexually abusing or exploiting them (both on and off-line exploitation).
* Exposure of minors to inappropriate commercial advertising
* Exposure to online gambling services
* Commercial and financial scams
* Impersonation and identity theft by exposure to so called phishing and vishing
* Threats through harmful programmes and software, virus’, malware and hacking

**Academic Freedom**

Everyone has the right to freedom of expression. This means everyone has the right to express lawful views and opinions freely, in speech or in writing, without interference from the state or other bodies carrying out public functions, including City College. This is true even when these views or opinions may offend, shock or disturb others. To ensure this, City College maintains an Academic Freedom Policy which includes the right to express views aloud through.

* Published articles, books or leaflets.
* Television or radio broadcasting
* Works of art
* The internet and social media

The College will not restrict debate or deliberation simply because the views being expressed may shock, offend or disturb others. In turn, the College expects all staff, students and stakeholders to show the same commitment by not obstructing or interfering with the rights of others to express views with which they might disagree.

**Cyber Bullying, Bullying and Harassment**

Cyber bullying - Is any form of bullying which takes place online or through IDMT. Some of the types of cyber bullying are outlined further below, however, this is not an exhaustive list. Any issues of cyberbullying, witnessed, reported or disclosed should be reported through the Bullying and Harassment policy

Harassment - Is the act of sending offensive, rude, and insulting messages and being abusive. Unwanted or solicited humiliating comments on posts, photos and in chat rooms. Being explicitly offensive whilst engaging with online gaming sites.

Denigration – Sending and sharing information about another person that is fake, damaging and untrue. Sharing photos of someone for the purpose to ridicule, spreading fake rumours and gossip. This can be on any site online or apps and may include altering photos of others and posting in online for the purpose of bullying.

Flaming – The use of really extreme, inflammatory and offensive language for the purposes of getting into online arguments and fights with the intention of getting another person into a state of distress.

Impersonation – Hacking into an email or social networking account and use the person's online identity to send or post vicious or embarrassing material to or about others. Activity could include making up of fake profiles on social media as well as other online accounts aimed at causing harm or distress.

Outing and Trickery – The sharing of personal information about another to trick someone into revealing personal information and images relating to themselves.

Cyber Stalking – The act of repeatedly sending messages that include threats of harm, harassment, intimidating messages, or engaging in other online activities that make a person afraid for their safety.

Exclusion –Intentionally leaving someone out of a group such as group messages, apps, social media groups, gaming sites and other online engagement.

**Social Media**

All staff and students, must also familiarise themselves about the risks and inappropriateness of sharing personal information about themselves via social media sites either with one another or within the wider public domain, understanding that any inappropriate material posted could affect their professional status. Staff and students should familiarise themselves with the mainstream Social media sites, their application and the associated risks, dangers and cyber-bullying implications with each site.

**Facebook**

Facebook is a popular free social networking website that allows registered users to create profiles, upload photos and video, send messages and keep in touch with friends, family and colleagues Facebook does not tolerate bullying and say they will remove bullying content when they become aware of it and may disable the account of anyone who bullies or attacks another. They have a set of community standards that they adhere to and it states that they will not tolerate:

* Pages that identify and intend to shame private individuals,
* Images altered to degrade private individuals,
* Photos or videos of physical bullying posted to shame the victim,
* Sharing personal information to blackmail or harass people
* Repeatedly targeting other people with unwanted friend requests or messages.

**Twitter**

Twitter is a 'microblogging' system that allows you to send and receive short posts called. Tweets. Tweets can be up to 140 characters long and can include links to relevant photos. Video, websites and resources. If users receive a tweet or reply that causes some form of harm or offence, that person can be ‘unfollowed’. If contact continues, the user in question can be blocked. A report may be sent to Twitter directly if further action is required.

**YouTube**

YouTube is a video sharing service that allows users to watch videos posted by other users and upload videos of their own. Users have a right to use YouTube without fear of being subjected to bullying or harassment. Bullying can be reported to You Tube and action taken when users breach their policies, intending to cause harm or distress. YouTube rules say content cannot be uploaded that contains; hate, nudity or graphic violence. If under comments, users are being bullied, harassed or threats are being made, they have a reporting tool page where reports are made for investigation.

**Instagram**

Instagram is an online photo sharing service. It allows users to apply different types of photo filters to pictures with a single click, then share them with others. Bullying or abuse on Instagram can happen in many ways. It can be either negative comments, fake profiles or hacking of accounts. Instagram take violations of their terms of service seriously, but their initial advice is to block and unfollow the person being abusive. However, if it continues or it has gotten worse, a direct report should be made.

**Snapchat**

Snapchat is a mobile app and service for sharing photos, videos, and messages with other users Cyber-bullying on Snapchat is likely to take the form of screenshots, sending pics without a users’ permission or posting negative comments with the intention to cause harm or distress

**WhatsApp**

WhatsApp Messenger is an online service that allows users to send instant messages, videos, photos, and short audio messages to either one person or within a group chat. Messages can only be sent to other smartphone users who also have WhatsApp. Once installed the app, checks the users address book for other WhatsApp users, and connects automatically. Users have to be over 16 legally. Bullying can take many forms as it is a messaging service. Users can be blocked and contacts deleted.

# Electronic images

Staff and students should not publish, share or distribute any electronic images outside of those relating to learning outcomes, where necessary, the College will obtain the student’s permission for use of a related electronic image. The College will not identify students in online electronic images or include the full names of students in the credits of any published materials.

The recording, taking and sharing of images, video and audio on any personal mobile device is to be avoided, except where it has been explicitly agreed with the student. Such authorised use is to be recorded. All mobile device use is to be open to monitoring scrutiny by the College

**The College Website**

The College takes overall responsibility to ensure that the website content is accurate, and the quality of presentation is maintained, and complies with statutory Office for Students (OfS) and Advertising Standards Authority (ASA) requirements. Where work is published or linked to another organisation the College will credit the sources used and state clearly the author's identity. Photographs published on the website do not have full names attached. Staff and student names are not used when saving or publishing electronic images in the file names or in the tags on the website or associated media

**Online Storage and Cloud Environments**

The College uses a secure cloud environment for the uploading and storing of information. Content is shared between different staff members and stakeholders according to their responsibilities e.g. all tutors upload information relating to their own students. Any electronic images uploaded to the online environment will only be accessible by members of staff only for the purposes of education.

**E-safety Complaints, Safeguarding and Prevent Concerns**

Any complaints about e-safety concerns should be progressed through the College complaints procedure or, in the case of a Safeguarding or Prevent issues, the Safeguarding and Prevent Policy. Under no circumstances should staff or students attempt to investigate a complaint themselves.

**Related Policies**

This policy needs to be read in conjunction with other policies including:

* Safeguarding Policy
* Whistleblowing Policy
* Academic Freedom Policy
* Health and Safety Policy
* Equality and Diversity Policy
* Safe Recruitment Policy
* Prevent Strategy
* Governance Code
* Bullying and Harassment Policy
* Complaints Policy and Procedure
* Student Disclaimer Policy
* Safe Recruitment Policy