

Online Safety Policy

Table of Contents

Scope of the Policy	2
Aim	2
Roles and Responsibilities	2
Policy Statements	3
Internet Usage	4
Use of the internet within the college	4
Student safety on the college internet system	4
Gaining access to the college internet	4
Mobile Phones, Tablets, Laptops and PDAs	5
Use of Digital and Video images	5
Social Media – Protecting Professional Identity	5
Communications	6
Unsuitable/Inappropriate activities	7
Responding to incidents of misuse	8
Inappropriate usage of internet	8
Handling online safety complaints	8
Communication of Policy	9
Social Media Postings	9
Useful information	9

Scope of the Policy

This policy applies to all members of Bird College (including staff, students, contractors, visitors, parents/carers) who have access to and are users of the college's ICT systems both in and out of Bird College.

The Education and Inspections Act 2006 empowers the Principal to such extent as reasonable, to regulate the behaviour of students when outside the Bird College site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, extremist behaviour, or other Online Safety incidents covered by this policy, which may take place outside of Bird College but are linked to membership of Bird College.

Aim

We recognise the value of the internet, email, social media and other technologies, and welcome their development. We continually strive to enhance their appropriate use (both within college and outside) in order to promote the technical and academic attainment and advancement of our students. We recognise within the Performing Arts sector that technology and Social Media can be an effective tool in engaging with other artists as well as future employers.

The technologies encompassed by this policy include all computer and Internet technologies and electronic communication devices such as mobile phones and tablets.

Roles and responsibilities

Board of Directors

The Board of Directors are responsible for approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by Directors receiving regular information about online safety incidents and monitoring reports. A member of Board has taken the role of the *Online Safety Director* combined with the role of Chief Executive Officer.

Principal and Artistic Director

The Principal has a duty of care for ensuring the safety (including online safety) of members of the Bird College community, though the day to day responsibility for online safety will be delegated to the Online Safety Coordinator.

Online Safety Coordinator/Designated Safeguarding Lead

The Online Safety coordinator is responsible for online safety issues and has a leading role in establishing and reviewing the college's online safety Policy. Other responsibilities will include:

- Ensuring that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place
- Providing advice for staff
- Liaising with the Local Authority/Relevant Body
- Liaising with the college's technical staff
- Writing online safety incident reports and creates a log of incidents to inform future online safety developments
- Meeting with the Online Safety Director to discuss current issues
- Reporting regularly to the Board of Directors

Network Manager/Technical Staff

* Bird College has a managed ICT service provided by Select technology Systems. It is the responsibility of Bird College to ensure that Select Technology Systems is fully aware of the college's Online Safety Policy and Procedures and that online safety measures are carried out by the technical staff.

The technical staff is responsible for ensuring:

- That the college's technical infrastructure is secure and is not open to misuse or malicious attack
- That the college meets the required online safety technical requirements
- That users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- Monitor and report on the college's firewall activity
- To provide log records when appropriate

Members of Staff

Are responsible for ensuring that:

- They have an up-to-date awareness of online safety matters and of the current Online Safety Policy and procedures
- They report any suspected misuse or problem to the Online Safety Coordinator
- All digital communication with students should be on a professional level and only carried out using the official college systems

Students

- Are responsible for using the digital technology systems in an appropriate manner
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Understand the factors that make students vulnerable to being drawn to into terrorism
- Should know and understand policies on the taking / use of images and on cyber-bullying

Policy Statements

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 online safety is therefore an essential part of college's online safety provision.

The online safety education will be provided in the following ways:

- Key online safety messages should be reinforced as part of the induction week and outlined again when the need occurs
- Students should be taught in all lessons to be critically aware of the materials / content they access online and be guided to validate the accuracy of information
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices

We believe that:

- Young people should never experience abuse of any kind
- Young people should be able to use the internet for education and personal development, but safeguards need to be in place to ensure they are kept safe at all times.

We recognise that:

- The online world provides everyone with many opportunities, however it can also present risks and challenges
- We have a duty to ensure that all young people and adults involved in our organisation are protected from potential harm online
- All young people, regardless of age, disability, gender reassignment, race, religion or belief, sex or sexual orientation, have the right to equal protection from all types of harm or abuse
- Working in partnership with young people, their parents, carers and other agencies is essential in promoting young people's welfare and in helping young people to be responsible in their approach to online safety.

Education and Training

It is important that all staff receive online safety training and understand their responsibilities, as outlined in this policy. A planned programme of formal online safety training will be made available to staff and provided by EduCare.

Internet usage

The internet is used within the college to raise standards, to promote student achievement, to support the professional work of staff and to enhance the college's management information and administration systems.

We recognise the importance of the internet as an essential element in modern education, business and social interaction. Access to the internet is therefore an entitlement for all staff and students and their responsibility is to use it with care.

Students will use the internet outside of college and part of our responsibility is to educate them in safe use of the technology.

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 experts in many fields for students and staff
- Professional development for staff through access to national developments, educational materials and effective professional practice
- Collaboration across support services and professional associations
- Exchange of curriculum and administration data within the college and any appropriate regulatory bodies

Student safety on the college internet system

- Students are educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Students are given guidance about personal safety including identity theft.

Gaining access to the college internet

- All students will be instructed in the appropriate and safe use of the internet during the induction process

- All staff must be aware of their responsibilities outlined in the staff handbook. If they have any concerns they should contact support@select-technology.co.uk

Mobile Phones, Tablets, Laptops and PDAs

- Students may use personal devices in and around the college to support their training and learning
- Students take full responsibility for the care and safety of their personal items and should always keep them secure and/or with them. Each student is allocated a locker and valuables boxes are provided in the studios.

Use of Digital and Video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that have recorded themselves or downloaded from the internet. However, staff and students need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet indefinitely and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry 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. 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 in the sharing, distribution and publication of those images
- Care should be taken when taking digital / video images ensuring 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 consent
- Photographs published on the 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

Social Media – Protecting Professional Identity

The college has a duty of care to provide a safe learning environment for students and staff. Staff members who harass, cyberbully, discriminate on the grounds of gender, race, or disability or who defame a third party may render the college liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The college provides the following measures to ensure reasonable steps are in place to minimise risk of harm to students, staff and the college through:

- Ensuring that personal information is not published
- Online Safety Training is provided

College staff should ensure that:

- They do not engage in online discussion on personal matters relating to members of the college community

- Personal opinions should not be attributed to the college

When official college social media accounts are established there should be:

- A process for approval by senior leaders
- Clear processes for the administration and monitoring of these accounts
- A code of behaviour for users of the accounts, including
- Systems for reporting and dealing with abuse and misuse
- Understanding of how incidents may be dealt with under the college disciplinary procedures

Communications

When using communication technologies, the college considers the following as good practice:

- The official college email service may be regarded as safe and secure and is monitored
- Users should be aware that email communications are monitored. Staff and students should therefore use only the college email service to communicate with others when in college, or on college systems (e.g. by remote access)
- Users must immediately report, to the Online safety Coordinator (Luisa Figuerola), in accordance with the college policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication
- Any digital communication between staff and students must be professional in tone and content. These communications may only take place on official (monitored) college systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Students should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies
- Personal information should not be posted on the college website and only official email addresses should be used to identify members of staff

Unsuitable/Inappropriate activities

The college believes that the activities referred to in the following section would be inappropriate in the college context and that users, as defined below, should not engage in these activities in / or outside the college when using the college equipment or systems. The college policy restricts usage as follows:

	User Actions	Acceptable	Acceptable at certain times	Acceptable for nominates users	Unacceptable	Unacceptable and illegal
Users shall not visit internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images					x
	Promotion or conduct of illegal acts					x
	Adult material that potentially breaches the Obscene Publication Act in UK					x
	Criminally racist material in UK					x
	Pornography				x	
	Promotion of any kind of discrimination				x	
	Threatening behaviour, including promotion of physical violence or mental harm				x	
	Promotion of extremism and terrorism					x
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the college or brings the college into disrepute				x	
	Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the college				x	
	Infringing copyright					x
	Revealing or publicising confidential or proprietary information				x	
	Creating or propagating computer viruses or other harmful files				x	
	File sharing			x		
Use of Social Media			x			
Use of video broadcasting e.g. YouTube			x			

Responding to incidents of misuse

Any incident of slander, abuse or defamation perpetrated on a social networking site which:

- impacts upon one of our students, shall be treated as bullying and shall be sanctioned in accordance with the college's Anti Bullying and Harassment Policy
- impacts upon one of our staff members, shall be treated as misconduct and shall be sanctioned accordingly
- impacts upon the reputation of the college, shall be treated as misconduct and shall be sanctioned accordingly

Inappropriate usage of internet

Inappropriate use of internet may result in suspension pending an investigation.

Handling online safety complaints

- Any complaint about staff misuse must be referred to the Online safety Coordinator
- Any complaint about student misuse must be referred to the Online safety Coordinator
- Complaints of a child protection nature must be dealt with in accordance with the college's safeguarding procedures

Communication of Policy

Students

- Students can find the Online Safety Policy on the College's website. The Policy is also available in a hard copy format
- Students are informed that Internet use will be monitored

Staff

- All staff are issued with this policy and its importance is explained. The policy can be found on *Breath*. The policy is also available in a hard copy format upon request.

Social Media Postings

All social media activity / postings in relation to work carried out at Bird College must always credit @birdcollegeuk and refer to the students / cast as Bird College's Students or Bird College Cast. Where possible the term MY or MINE is to be avoided. No videos are to be posted without permission from the Joint Principal & Artistic Director.

Useful information:

NSPCC cyberbullying page

- <https://www.nspcc.org.uk/preventing-abuse/child-abuse-and-neglect/bullying-and-cyberbullying/>

Childline cyberbullying page

- <https://www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety/>

ThinkUknow

- <https://www.thinkuknow.co.uk/>

ThinkUknow – How to Report

- https://www.thinkuknow.co.uk/8_10/report/

BullyingUK

- <http://www.bullying.co.uk/general-advice/bullying-at-university/>

Government link to report online material promoting terrorism or extremism

<https://www.gov.uk/report-terrorism>

Document Control

Document title: **Online Safety Policy**

Version	Author		Reviewed/Authorised	
	By	Date	By	Date
1.1	Matt Elliot	29.07.13	Unknown	29.07.13
1.2	Matt Elliot	10.04.16	Unknown	10.04.16
1.3	Luisa Figuerola	19.07.17	BOD	20.03.18
1.4	Luisa Figuerola	19.07.17	Luisa Figuerola	29.07.19
1.5	Luisa Figuerola	29.06.21	Luis De Abreu	02.07.21
1.6	Luisa Figuerola	22.07.2024	Luis De Abreu	22.07.2024

Issue: 1.6
 Date of current issue: 22.07.2024
 Date of next review: 22.07.2025