**e-Safety Policy**

Bodywork Company Performing Arts

January 2021

**Contents**

* The background to this policy
* Rationale
* The e-safety curriculum
* Continued Professional Development
* Monitoring, and preventing e-safety incidents
* Responding to e-safety incidents
* Appendices (including AUPs)

**Background to this policy:**

The purpose of this policy is to describe the safeguarding measures in place for adults and young people in College in relation to e-safety, including:

* The policies and practice embedded in our College and followed by the whole College community
* The infrastructure and how it is set up to keep students safe online, including monitoring, and preventing and responding to e-safety incidents

e-safety in College is primarily a safeguarding issue and not a computing / technology one. Therefore this policy should be viewed alongside other Safeguarding policies and approaches including, but not limited to:

* [Professional boundaries in relation to your personal internet use and social networking online – advice to staff (LSCB)](http://www.cambridgeshire.gov.uk/lscb/)
* Safeguarding and Child Protection
* Personal Social and Health Education (PSHE)
* Safer Working Practices
* Data Protection Policy
* Anti-Bullying Policy
* College Complaints Procedure
* [Cambridgeshire Progression in Computing Capability Materials](http://www.ccc-computing.org.uk)
* Whistle Blowing Policy

This policy must be read alongside the staff and student Acceptable Use Policies attached as appendices. These AUPs outline the expectations and sanctions which apply to staff and students use of technology.

* The development of our safety policy involved:
  + The Designated Person for Child Protection
  + Cambridgeshire Local Authority Advisor (Cambridgeshire Education ICT Service)
  + The governor responsible for Safeguarding

It was ratified by the Chair of Governors on 24th June 2019 and will be formally reviewed in on 22nd January 2021

* This policy may also be partly reviewed and / or adapted in response to specific e-safety incidents or developments in the College’s use of technology. It has been shared with all staff and students via email and it is on the College website.
* All staff and students must be familiar with this policy and all staff and students must sign the relevant Acceptable Use Policy before being allowed to access College systems (see appendices). As E-safety is an important part of strategic leadership within the College, all staff have a shared responsibility to ensure that the policy and practices are embedded. This will be monitored by the Principal, the Designated Person for Child Protection and Governors.

**Rationale:**

* At Bodywork Performing Arts, *which hereafter will be referred to as the College*, we believe that the use of technology in College brings great benefits. To live, learn and work successfully in an increasingly complex and information-rich society, our students must be able to use technology effectively.

The use of these exciting and innovative technology tools in College and at home has been shown to support learning and promote student achievement. Yet at the same time, we recognise that the use of these new technologies can put young people at risk within and outside the College.

The risks they may face can broadly be categorised into the ‘3 C’s’ **Contact**, **Content** and **Conduct** (Livingston and Haddon) and may include

* Access to harmful, illegal or otherwise unsuitable content including gaming, gambling sites, sexually explicit material and websites with extremist ideologies and images consistent with the Prevent Strategy
* Unauthorised access to / loss of / sharing of personal information
* The risk of being subject to grooming by those with whom they make contact on the internet
* The sharing / distribution of personal images without an individual’s consent or knowledge
* Inappropriate communication / contact with others
* Cyber-bullying
* An inability to evaluate the quality, accuracy and relevance of information on the internet
* Plagiarism and copyright infringement
* Illegal downloading of music or video files
* The potential for excessive use which may impact on the social and emotional development and learning of the young person.

While students and young people need support to keep them safe online, the risks associated with the use of technology are not restricted to just them. E-Safety issues can also affect adults who work or are associated with the College and this will be referenced in more detail later in this policy.

Technologies regularly used by students and staff include:

Staff:

* Staff laptops and also desktops in the office and ICT Suite including staff level internet access and server access.

Students:

* Desktops in the ICT Suite including filtered access to the Internet

Where the College changes the use of existing technology or introduces new technologies which may pose risks to student’s safety, a risk assessment will be completed to show how the risk is being mitigated and reduced to an acceptable level.

**The e-Safety curriculum:**

When using online technologies, it is essential that students understand how to behave in a safe and responsible manner and also how to react when faced with inappropriate content or situations which make them feel uncomfortable. The students are taught to

* Use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact.

This is achieved using a combination of:

* Our programme for e-safety education is evidenced in teachers’ planning either as discrete or embedded activities.
* Key e-safety messages are delivered and reinforced through cross curricular opportunities such as emailing, researching, blogging and communicating in discussion forums.

**Continued Professional Development:**

* Staff at the College receive up-to-date information and training on e-Safety issues in the form of staff meetings, email updates and updates from the designated Safeguarding Lead, as well as training from external providers where appropriate.
* New staff receive information on the College’s acceptable use policy as part of their induction, including advice on Protecting their Professional Reputation Online.
* All staff have been made aware of individual responsibilities relating to the safeguarding of students within the context of e-Safety and know what to do in the event of misuse of technology by any member of the College community.

**College website:**

The main purpose of our College website is to provide information. Our College website will not only tell the world that our College exists, but it will provide information for our students and parents, (current and prospective) and publish the statutory information required by the Department for Education.

Under safeguarding responsibilities, it is the duty of the College to ensure that every child/young person in our care is safe. The Principal and the Governing Body therefore take on the responsibility to ensure that no individual can be identified or contacted either via, or as a result of, a visitor using the College website.

The College should establish clear policies to ensure that its website is maintained, is effective, and does not compromise the safety of the students or staff.

**Monitoring, and averting e-safety incidents:**

The College keeps students safe when using online technologies through a combination of e-safety education, filtering and monitoring student’s online activity and reporting incidents, including following Child protection procedures where appropriate.

The College’s technology infrastructure is designed to minimise the risks associated with adult and student use of technology. This is provided by Midshire. Filtering and an anti-virus package is in place, with:

* Secure, private CPSN provided internet connection to each College with a direct link to the National Education Network. Managed firewalling.
* Restrictions on download of software, apps and file types from known compromised sites

A system of staff passwords is in place to enable appropriate access to the College network.

* Permanent staff members have individual, password protected logins to the College network.
* The College’s network can either be accessed using a wired or wireless connection. However, the wireless network is encrypted to the standards advised by the Local Authority and the wireless key is kept securely by the College office.

Whilst we recognise that it is impossible to totally eliminate the risks associated with the use of technology, these safeguards are in place to help minimise these risks as much as possible.

**Responding to e-safety incidents:**

It is important that all members of staff – teaching and non-teaching – are aware of how to respond if an e-safety incident occurs or they suspect a child is at risk through their use of technology.

* Staff responses to e-safety incidents must be consistent with responses to other incidents in College. This may mean that serious actions have to be taken in some circumstances.
* If an e-safety incident occurs, the College will follow its agreed procedures for responding including internal sanctions and involvement of parents (this may include the deactivation of accounts or restricted access to systems as per the College’s AUPs.

In addition, the Education and Inspections Act 2006 empowers Principles to such extent as is reasonable, to regulate the behaviour of students when they are off the College site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents which may take place outside of the College but has an impact within the College community.

* With this in mind, the Principal may decide to apply the sanctions and / or procedures in the relevant AUP to incidents which occur outside of College if she deems it appropriate.

The Education Act 2011 gives College staff the powers, in some circumstances to search personal digital devices and decide whether or not to delete data or files if the person thinks there is good reason to do so.

However, there is a risk that this could conflict with guidance about dealing with incidents where a child or young person may be at risk where it may be inadvisable to delete, save or share content. The College will, where appropriate, seek ways to resolve areas of concern with parents before taking any further action

Where the College suspects that an incident may constitute a Child Protection issue, the usual Child Protection procedures will be followed. This process is illustrated in the diagram below.

