ATRIUM
STUDIO
atrium-studio.co.uk

E-Safety Policy

Document produced by: Matt Messias, The Principal

Date produced: May 2015

Adopted by Governing Body: TBA

To be reviewed: May 2018

1.1 WHAT IS E-SAFETY?

The Atrium Studio’s E-Safety Policy reflects the need to raise awareness of the safety issues associated with information systems and electronic communications as a whole.

E-Safety encompasses not only Internet technologies but also electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits, risks and responsibilities of using information technology. It provides safeguards and raises awareness to enable users to control their online experiences.

The Internet is an unmanaged, open communications channel. The World Wide Web, e-mail, blogs and social networking all transmit information using the Internet’s communication infrastructure internationally at low cost. Anyone can send messages, discuss ideas and publish material with little restriction. These features of the Internet make it an invaluable resource used by millions of people every day.

Much of the material on the Internet is published for an adult audience and some is unsuitable for students. In addition, there is information on weapons, crime and racism access to which would be more restricted elsewhere. Students must also learn that publishing personal information could compromise their security and that of others. Schools need to protect themselves from legal challenge. The law is catching up with Internet developments: for example it is an offence to store images showing child abuse and to use e-mail, text or Instant Messaging (IM) to ‘groom’ children.

Schools can help protect themselves by making it clear to students, staff and visitors that the use of Atrium Studio equipment for inappropriate reasons is “unauthorised”. However, Schools should be aware that a disclaimer is not sufficient to protect a School from a claim of personal injury and the School needs to ensure that all reasonable actions have been taken and measures put in place to protect users.

1.2 RESPONSIBILITIES OF STAFF

Information technologies are developing rapidly and can leave staff unsure of best practice or how to discuss E- Safety issues with students. The trust between students and Atrium Studio staff is essential to education but very occasionally it can break down. Nationally, CEOP has been set up by the Home Office to “safeguard children’s online experiences and relentlessly track down and prosecute offenders”. A member of staff who flouts security advice, or uses e-mail or the Internet for inappropriate reasons risks dismissal.

1.3 E-SAFETY FOR STUDENTS WITH ADDITIONAL NEEDS

There is an underlying assumption that children have both understanding and application of “safety”. Students need to understand that rules given to them must be followed. Students need to learn safety rules in a way that does not frighten them and which gives them confidence to know what to do in certain situations. Students need to understand that certain rules will change and develop as they get older

Students need to learn how to apply strategies that will help them to avoid certain “risks” such that they need to plan ahead.

There are certain aspects of the above that are particularly challenging for students with additional needs and children who we may consider to be vulnerable in this learning context. Students will clearly have individual needs that will present a range of issues when teaching E-Safety but some common difficulties may be:

- They may be still developing their social understanding of safety and so may relate better to strategies used with younger children
- They are likely to find it hard to apply the same rules in different situations
- Most safety principles rely on children being able to explain what happened or to ask for help
- Some children may have poor recall and difficulties with learning through experience.
- It would seem to be appropriate, therefore, that this policy may need to be adapted to meet the needs of all of our students during an academic year if needs should change.

This may take the form of child-focused strategies that would apply to a student with specific needs and would be made available to all staff involved in Internet use with that child. Alternatively, whole School approaches could take into consideration strategies that would support the needs i.e. specific choices of visual support to remind students of the rules. Advice and guidance can be sought from the safeguarding officer.

In writing this E-Safety policy, we have considered these issues:

Guided educational use
Curriculum Internet use produces significant educational benefits including access to information from around the world and the ability to communicate widely and to publish easily. Curriculum Internet use should be planned, task- orientated and educational within a regulated and managed environment in order to enrich and extend learning activities. Directed and successful Internet use will also reduce the opportunities for activities of little education value. Staff should guide students in on-line activities that will support the learning Atrium Studio planned for the students' age and maturity.

Risk assessment
21st century life presents dangers including violence, racism and exploitation from which children and young people need to be protected. At an appropriate age they will need to learn to recognise and avoid these risks – to become "internet-wise".

We need to perform risk assessments to ensure that our students are fully aware of and can mitigate risks of Internet use. Students need to know how to cope if they come across inappropriate material.

Students may access the Internet in Youth Clubs, Libraries, public access points and in homes. Where possible we will take a lead to help guide staff and parents by offering support and development opportunities.

Responsibility
E-Safety depends on staff, Schools, governors, advisers, parents and - where appropriate - the students themselves taking responsibility. Staff have a particular responsibility to supervise use, plan access and set good examples. The balance between educating students to take a responsible approach and the use of regulation must be judged carefully.

Regulation
The use of a finite and expensive resource, which brings with it the possibility of misuse, requires regulation. In some cases, access must simply be denied, for instance un-moderated chat rooms present immediate dangers and are usually banned. Fair rules, clarified by discussion and prominently displayed at the point of access will help students make responsible decisions.

The IT support technician will keep an up-to-date record of access levels granted to all network users. Parents should be informed that students will be provided with supervised Internet access and parents and students should sign an acceptable use agreement. The Leadership Team Member with overall responsibility for ICT will take responsibility for regularly checking that filtering and monitoring is appropriate, effective and reasonable, and that technical staff have not taken on themselves the responsibility for educational or disciplinary issues. Filtering software is used in place and will provide a level of access to the internet in line with acceptable School use.

Appropriate strategies
This policy describes strategies to help to ensure responsible and safe use. They are based on limiting access, developing responsibility and on guiding students towards educational activities. There are no straightforward or totally effective solutions and staff, parents and the students themselves must remain vigilant. The Atrium Studio will take all reasonable precautions to ensure that users access only appropriate material. Filtering strategies will be selected, in discussion with the filtering provider where appropriate. The filtering strategy will be matched to the age and curriculum requirements of the Student.

Principles behind Internet use
The purpose of Internet use in school is to raise educational standards, to promote student achievement, to support the professional work of staff and to enhance the School's management information and business administration systems. Internet access is an entitlement for students who show a responsible and mature approach to its use. The Atrium Studio has a duty to provide students with safe and secure Internet access as part of their learning experience. The Atrium Studio's Internet access should be designed expressly for student use and will include filtering appropriate to the age of the student.

Students will be taught what is acceptable and what is not and given clear objectives for Internet use. This will be delivered after staff have received E-Safety training and the teaching materials developed with CEOP's guidance. A proportion of tutor time will be spent teaching the students E- Safety strategies and time allowed for developmental discussion to raise awareness and impart knowledge and understanding.

Safety education
Students will be educated in the responsible and safe use of the Internet and other technologies through a range of strategies including:

- Reactive discussion when a suitable opportunity occurs.
- We will ensure that the use of Internet derived materials by staff and by students complies with copyright law, students will be made aware of plagiarism and issues relating to work research being undertaken for coursework. Staff and students will be trained to become critically aware of the materials they read and shown how to validate information before accepting its accuracy. Students will be taught to acknowledge the author of the information used and to respect copyright when using Internet material in their own work.
- Staff and student electronic communications
- Staff and students need to understand that the use of the School's network is a privilege which can be removed should a good reason arise. The School will monitor all network and Internet use in order to ensure student safety.
- Visiting speakers through the SMSC programme.

1.4 RESPONSE TO AN INCIDENT OF CONCERN

Internet technologies and electronic communications provide children and young people with opportunities to broaden their learning experiences and develop creativity in and out of School. However, it is also important to consider the risks associated with the way these technologies can be used.

The E-Safety Policy recognises and seeks to develop the skills that children and young people need when communicating and using these technologies properly, while keeping safe and secure, and acting with respect for others.

These risks to E-Safety are caused by people acting inappropriately or even illegally. Any potential issue must be dealt with at a personal level. Teachers are the first line of defence; their observation of behaviour is essential in detecting danger to students and in developing trust so that issues are reported. Incidents will vary from the prank or unconsidered action to considered illegal activity. Incidents will be dealt with as per the school's discipline policy.

This section will help staff determine what action they can take and when to report an incident of concern to the Safeguarding Officer. Matters can then be handed over to the Children's Safeguards Service or the Police if that becomes necessary.

What does electronic communication include?

- Internet collaboration tools: social networking sites and web-logs (blogs) Internet research: websites, search engines and web browsers
- Mobile phones and personal digital assistants (PDAs) Internet communications: e-mail and IM
- Webcams and videoconferencing Wireless games consoles

What are the risks?

- Receiving inappropriate content Predation and grooming
- Requests for personal information Viewing 'incitement' sites
- Bullying and threats Identity theft
- Publishing inappropriate content Online gambling
- Misuse of computer systems Publishing personal information
- Hacking and security breaches Corruption or misuse of data

Implementation and Compliance

No policy can protect students without effective implementation. It is essential that staff remain vigilant in planning and supervising appropriate, educational ICT experiences. The following ideas and checks may be implemented:

- The quick audit provided in the Core E-Safety Policies is a good place to start when checking the School's E- Safety readiness.
- How are students reminded of their responsibilities? Displaying posters in rooms with computers is one useful approach.
- Do staff, students and parents know how to report an incident of concern regarding Internet use?
- Where filtering is managed locally, does a senior leader approve the Atrium Studio filtering configuration and supervise the staff who manage the filtering system?

2.1 TEACHING AND LEARNING

2.1.1 Why is Internet use important?

The purpose of Internet use in South Devon Atrium Studio is to raise educational standards, to promote student achievement, to support the professional work of staff and to enhance the School's management functions. Internet use is part of the statutory curriculum and a necessary tool for learning.

Students use the Internet widely outside School and will need to learn how to evaluate Internet information and to take care of their own safety and security.

2.1.2 How does Internet use benefit education?

Benefits of using the Internet in education include:

- access to world-wide educational resources including museums and art galleries;
- cultural exchanges between students world-wide;
- vocational, social and leisure use in libraries, clubs and at home;
- 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;
- collaboration across support services and professional associations;
- improved access to technical support including remote management of networks and automatic system updates;
- to learning wherever and whenever convenient.

Staff will be able to access the internet for their own professional development and professional responsibilities associated with their role.

2.2 MANAGING INFORMATION SYSTEMS

2.2.1 The maintenance of information system security Local Area Network security:

- Users must act reasonably – e.g. the downloading of large files during the working day will affect the service that others receive.
- Users must take responsibility for their network use.
- Workstations are secured against user mistakes and deliberate actions.
- Servers are located securely and physical access restricted to the IT Support staff directly employed in this team.
- The server operating system is secured and kept up to date.
- Virus protection for the whole network must be installed and current.
- Access by wireless devices is pro-actively managed.

Wide Area Network (WAN) security:

- All Internet connections are arranged by the Atrium Studio to ensure compliance with the security policy.
- Firewalls and switches are configured to prevent unauthorized access.
- The security of the School information systems will be reviewed regularly.
- Virus protection will be updated regularly.
- Personal data sent over the Internet will be encrypted or otherwise secured.
- Portable media may not be used without specific permission followed by a virus check.
- Unapproved system utilities and executable files will not be allowed in students' work areas or attached to e-mail.
- Files held on the School's network will be regularly checked.
- The network manager will review system capacity regularly.

2.2.2 The management of e-mail

- Students may only use approved e-mail accounts.
- Students must immediately tell a teacher if they receive offensive e-mail.
- Students must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Access in School to external personal e-mail accounts is blocked.
- Excessive social e-mail use by students can interfere with learning and may be restricted.
- The School's e-mail system must NOT be used for social use.
- E-mail sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on School headed paper.

3.0 E-SAFETY CONTACTS AND REFERENCES

Childline http://www.childline.org.uk
Child Exploitation & Online Protection Centre http://www.ceop.gov.uk http://www.thinkuknow.co.uk/
Internet Watch Foundation: http://www.iwf.org.uk/
Kidsmart; http://www.kidsmart.org.uk/
NSPCC: http://www.nspcc.org.uk/html/home/needadvice/needadvice.htm
Virtual Global Taskforce – Report Abuse: http://www.virtualglobaltaskforce.com/