The Derby High School
POL004
E Safety Policy

2016-17

Audience: Public

E SAFETY POLICY

OUTLINE

New technologies have become integral to the lives of our students in today's society both within School and in their lives outside. The internet and other digital and information technologies open new opportunities for learning and our students should have an entitlement to safe internet access at all times. An effective e-safety policy should help to ensure safe and appropriate use.

Use of these new technologies can put students at risk within and outside School. These include:

- access to illegal, harmful or inappropriate images or other content.
- unauthorised access to/loss of/sharing of personal information.
- the risk of grooming by those with whom they make contact on the internet.
- the sharing/distribution of personal images without the individual's consent or knowledge.
- inappropriate communication/contact with others including strangers.
- cyber-bullying.
- access to unsuitable video/internet games.
- inability to evaluate the quality, accuracy and relevance of information on the internet.
- plagiarism or copyright infringement.
- illegal downloading of music or videos.
- the potential for excessive use, impacting on social or emotional development.
- the risk of grooming related to extremist/terrorist organisations

It is impossible to eliminate these risks but important to assist students to have the confidence and skills to deal with these issues, such that they remain responsible users and stay safe.

RATIONALE

The scope of this Policy applies to all members of the School community – staff, students, volunteers, parents/carers, visitors and community users - who have access to and are users of School ICT systems both in and out of School.

REVISION LOG

Change Date	Reason for change	Details	Approved By
Spring 2014	Document Created	First Revision	School Governing Body
Spring 2015	Annual Review		School Governing Body
Spring 2016	Annual Review		School Governing Body
Spring 2017	Annual Review		School Governing Body

ROLES AND RESPONSIBILITIES

GOVERNORS

Governors are responsible for the approval and review of the Policy. This will be carried out through the Governors Buildings and Health and Safety subcommittee. A member of the Governing Body will have responsibility for e-safety as part of their responsibilities regarding safeguarding.

DEPUTY HEADTEACHER

The Deputy Headteacher is responsible for ensuring;

- routines for monitoring and staff training.
- arrangements for the management of a serious e-safety incident

TEACHING, SUPPORT STAFF, ICT SUPPORT STAFF

- the School ICT infrastructure is secure and not open to misuse or attack.
- the School Acceptable Use Protocol is adhered to.
- security arrangements are adhered to.
- they participate in relevant CPD, including e-safety and related Child Protection issues.
- they report any issue for investigation.
- students understand and follow e-safety advice.
- students understand the concept of plagiarism and copyright regulations.
- they are aware of e-safety issues related to mobile telephones, cameras and any other hand held devices.
- guidance to sites that have been previously checked for any unsuitable material.
- digital communications with students and parents should adhere to proper professional standards

STAFF

ELECTRONIC COMMUNICATION WITH PUPILS

(ALSO SEE THE- 'PROFESSIONAL RELATIONS' POLICY)

No e-mail communication should occur which does not pass through the school network mails boxes and addresses. Staff, workers and volunteers should not participate in chat rooms, Twitter, MSN, Instagram, online gaming (or any social networking sites yet to be created) with any pupils irrespective of age or with former pupils under the age of 18. In particular, staff, workers and volunteers should neither accept nor request pupils or former pupils under the age of 18 as friends on Facebook or other social networking sites. Staff, workers and volunteers should be mindful of the impact on younger siblings or friends of former pupils in any social contact. No text or instant messaging conversation should take place between staff, workers and volunteers and a pupil. In the event of this happening it should be recorded and placed on the pupil's file.

USE OF SOCIAL NETWORKING SITES (ALSO SEE THE- 'PROFESSIONAL RELATIONS' POLICY)

Staff, workers and volunteers using social networking sites in a personal capacity should ensure that they do not conduct themselves in a way that is detrimental to the school. For example they should not:

- allow interaction on websites to damage or compromise working relationships with colleagues.
- post photographs of themselves, colleagues or students taken in school
- post or sending abusive or defamatory messages
- record any confidential information about school on any social networking site
- post information which will disclose the identity of a student.

STUDENTS

Students are:

- responsible for using the ICT systems in accordance with School acceptable use guidance, which they will be given prior to use of the system. The acceptable use guidance also appears on all school computer sign in pages.
- expected to respect copyright and avoid plagiarism.
- expected to report abuse.
- expected to avoid misuse, including cyber-bullying and misuse of images.
- expected to know how to keep themselves safe on the internet.

PARENTS/CARERS

Parents and Carers are expected to support School Policies in relation to e-safety.

AIMS AND OBJECTIVES

AIM 1 – TO MAKE CURRICULUM PROVISION FOR E-SAFETY

Objective:

1. A planned programme of e-safety teaching will be made as part of PSHCE covering the use of ICT and wider technologies.
2. Key e-safety and cyberbullying awareness messages will be reinforced as part of assemblies and Form time.
3. Students should be taught to be critically aware of on-line materials and content.
4. Responsible use of ICT should be promoted, including reporting of incidents of concern.
5. Students should be taught to respect copyright and acknowledge sources.

AIM 2 – PROMOTING E SAFETY WITH PARENTS/CARERS

Objective:

1. Guidance regarding e-safety is available to parents/carers on the school website.
2. The management of any pastoral issues involving the use of the internet or other technologies should include appropriate advice to parents regarding e-safety.

AIM 3 – SECURE TECHNICAL PROVISION WILL BE ESTABLISHED IN RELATION TO ALL COMPUTER PROVISION AND OTHER TECHNOLOGIES USED IN SCHOOL

Objective:

1. Computer infrastructure, equipment, filtering and monitoring will meet relevant Local Authority guidance.
2. There will be an annual audit of e-safety in School.
3. Technical equipment will be securely located with restricted access.
4. All users will have clearly defined access rights to School ICT systems.
5. All users will be provided with a username and password.
6. 'Master' or administrative passwords will be restricted.
7. To ensure students or staff do not visit unacceptable or illegal sites.

AIM 4 – AS PART OF SAFEGUARDING TRAINING, PROVIDE ALL STAFF WITH SPECIFIC E SAFETY TRAINING

Objective:

1. Annual provision will be made for e-safety training for all staff. This provision will be extended to members of the Governing Body where possible.
2. E-safety training will form part of the induction of new staff to the School.
3. Students should be educated in the risks associated with using digital images, in particular the publication of the images of self on the internet.

AIM 5 – TO ENSURE THE SAFE KEEPING OF PERSONAL DATA, MINIMISING THE RISK OF ITS LOSS OR MISUSE

Objective:

1. To comply with all requirements of the Data Protection Act 1998 ensuring that personal data must be:
   - fairly and lawfully processed.
   - processed for limited purposes.
   - adequate, relevant and not excessive.
   - accurate.
   - kept no longer than is necessary.
   - processed in accordance with the data subject's rights.
   - secure.
   - only transferred to others with adequate protection.
2. Use personal data only on secure protected computers, ensuring that the computer is properly 'logged off' when personal data has been used.
3. Transfer data in secure settings.

AIM 6 – TO ENSURE SECURE COMMUNICATION FOR PROPER PROFESSIONAL AND SCHOOL APPROVED PURPOSES

Objective:

1. To maintain a safe and secure School e-mail service that may be monitored.
2. To promote students and staff to immediately report any offensive, threatening or bullying communication.
3. To ensure that any digital communication between staff and student is professional in tone and content.
4. To restrict the use of mobile telephones for students with the use of personal e-mail addresses and social networking sites being banned.

POLICY MONITORING AND EVALUATION

Evaluation of policy will include:

- logs of reported incidents.
- any data on network activity.
- annual evaluation of this curricular provision.
- Student Voice.
- Parent Voice.

RELATED DOCUMENTS

- Acceptable use policy- students/staff
- Anti- Bullying policy (Students)
- Child protection policy (Staff)
- Professional relations policy (Staff)