

E-Safety policy

Date of approval by Governors: December 2015 Next review date: December 2016

E-SAFETY POLICY

1. INTRODUCTION

Our policy applies to all students, staff, governors and volunteers associated with Great Sankey High School.

The 'staying safe' outcome of Every Child Matters is at the heart of the policy.

The 'staying safe' outcome includes aims that young people are:

- safe from maltreatment, neglect, violence and sexual exploitation
- · safe from accidental injury and death
- safe from bullying and discrimination
- safe from crime and anti-social behaviour in and out of school
- secure, stable and cared for.

Most of the above aims apply equally to the 'virtual world' that young people will encounter whenever they use ICT in its various forms. For example, we know that the internet has been used for grooming young people with the ultimate aim of exploiting them sexually; we know that ICT can offer new weapons for bullies, who may torment their victims via websites or text messages; and we know that young people have been exposed to inappropriate content when online, which can sometimes lead to their involvement in crime and anti-social behaviour.

It is the duty of Great Sankey High School to ensure that every student in our care is safe, and the same principles should apply to the 'virtual' or digital world as would be applied to the school's physical infrastructure.

The main areas of this policy are:

- 1. Definitions
- 2. The Current Technologies
- 3. The E-Safety Risks
- 4. Strategies to Minimise the Risks
- 5. Acknowledgement of Copyright
- 6. Review

7. This policy should be read in conjunction with the school safeguarding policy, guidance for staff about social media published in the staff handbook and the social media protocols for school branded social media sites.

2. DEFINITIONS

Inappropriate Material is understood by us to be:

• Online games featuring unacceptable violence.

- Content of a risqué nature.
- Material intended for a mature audience
- Material not intended for an academic environment.

Undesirable Materials

- Pornographic Images or obscene text
- Language that is abusive, profane, inflammatory, coercive, defamatory, blasphemous or otherwise offensive on web sites or in e-mail messages.
- Racist, homophobic, exploitative or illegal material or messages on web sites or in e-mail.
- Material which promotes any other illegal / antisocial activity.

Undesirable Contacts

• E-mail messages from unknown or unverified parties who seek to establish a student's identity and/or to communicate with the student for potentially criminal purpose.

Unacceptable Use

- Deliberate searching for and access to undesirable materials.
- Creating and transmitting e-mail messages that contain unacceptable language or content.
- Creating and publishing Internet materials that contain unacceptable language and content.

3. CURRENT TECHNOLOGIES

ICT in the 21st Century has an all-encompassing role within the lives of young people and adults. New technologies are enhancing communication and the sharing of information. Current and emerging technologies used in school and, more importantly in many cases, used outside of school by students include:

- Internet
- e-mail
- Instant messaging often using simple web cams
- Blogs (an on-line interactive diary)
- Podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player)
- Social networking sites
- Video broadcasting sites
- Chat Rooms
- Gaming Sites
- Music download sites
- Smart phones with e-mail, web functionality and cut down 'Office' applications.
- Mobile phones with camera and video functionality
- Mobile technology (e.g. games consoles) that are 'internet ready'.

4. E-SAFETY RISKS

The risks can be summarised under the following headings identified in BECTA's Safeguarding Children in a Digital World (2006) advice:

- Exposure to age-inappropriate material
- Exposure to inaccurate or misleading information
- Exposure to socially unacceptable material, such as that inciting violence, hate or intolerance
- Exposure to illegal material, such as images of child abuse
- Grooming using communication technologies, leading to sexual assault
- Exposure of minors to inappropriate commercial advertising
- Exposure to online gambling services
- Commercial and financial scams
- Bullying via websites, mobile phones or other forms of communication device
- Downloading of copyrighted materials e.g. music and films

4.1 GREAT SANKEY HIGH SCHOOL STRATEGIES TO MINIMISE THE E-SAFETY RISKS

- e-safety issues are covered, where appropriate, across the curriculum.
- e-safety implications of social networking internet sites are highlighted in particular, parents are asked to take note that 13 is the minimum age for sites such as facebook. Where we encounter issues on sites such as facebook where the user is not 13 we will report it.
- e-safety material sent home to parents on a periodic basis as part of Contact
- e-safety advice made available on the school web site and the CEOP report abuse is on the site
- e-safety notice to be displayed near the PC located in each classroom.
- e-safety included as a theme in assembly programmes
- mobile phone use by students is restricted on school the premises.
- internet filtering at a school level.

It is Great Sankey High School's policy that every reasonable step should be taken to prevent exposure of students to undesirable materials on the Internet. It is recognised that this can happen not only through deliberate searching for such materials but also unintentionally when a justifiable Internet search yields unexpected results.

Unintentional access of undesirable internet material by students

Should students be unintentionally exposed to undesirable materials the following steps will be taken:

- Pupils should notify a teacher immediately.
- The teacher in charge should notify the Headteacher and network manager/ Technician

- The network manager/ Technician will add the web site URL to the local internet blocked site list
- At the discretion of the Headteacher a student's parents/guardian and/or School
- Governors should be informed depending on the seriousness of the incident.

Intentional access of undesirable materials by students

Should students intentionally seek to access undesirable material the following steps will be taken:

- The teacher in charge should notify the Headteacher and Network manager / Technician.
- The Network manager / Technician will add the web site URL to the local internet blocked site list
- The incident will be treated as a disciplinary matter and at the discretion of the Headteacher a student's parents/guardian and/or School Governors should be informed depending on the seriousness of the incident. Students may have their access to the internet and / or computers restricted for a period of time.
- Repeated, flagrant or habitual intentional access of such material will be treated as a serious disciplinary issue.
- Senior management, parents and the governing body will be advised.

4.2 Access of inappropriate material by students

There may be occasions when students access a web site which is considered to be inappropriate but which does not necessarily fall into the "undesirable materials" category.

In such circumstances the Network manager or Technician should be advised and access to the site will be blocked.

Supervision of Students

As a further precaution against the accessing of unsuitable material by students – computer use should be supervised by a member of teaching or support staff.

Deliberate access to undesirable materials by adults

Deliberate access to undesirable materials by adults is unacceptable and will be treated as a disciplinary issue.

If abuse is found to be repeated, flagrant or habitual the matter will be treated as a very serious disciplinary issue.

The Governors will be advised and the LA consulted.

Receipt and transmission of e-mails by students

It is recognised that e-mail messages received or transmitted by students can contain language or content that is unacceptable.

It is also recognised that some people may try to use e-mail to identify and contact students for unacceptable reasons.

To avoid these problems Great Sankey High School uses an Internet e-mail service that guarantees the bona-fide nature of the school e-mail communicants.

The use of private email in school by students is discouraged.

If staff believe that a student has been targeted with e-mail messages by parties with criminal intent the messages will be retained, the incident recorded the Governors student's parents and police, where appropriate, informed.

Publishing of materials on the Internet

It is recognised that staff and students may at sometime produce and publish materials on an Internet web site associated with the school.

No material will be published on the Internet which contains any unacceptable images, language or content.

No written or photographic material will be published on the internet, which will reveal the identity of any student.

Use of the School Internet by visitors and guests

Members of the school staff will take responsibility for the actions of any adult guests or visitors to whom they allow use of the school's Internet facilities.

The essential "dos and don'ts" should be explained to such guests and visitors prior to their use of the Internet.

Information will also be provided on the school's virtual learning environment.

Unacceptable use will lead to the immediate withdrawal of permission to use the school's Internet facility.

5. ACKNOWLEDGEMENT OF COPYRIGHT

It is recognised that all materials on the Internet are copyright unless copyright is specifically waived.

It is the school's policy that the copyright of Internet materials will be respected.

Material published on the Internet as part of a staff member's professional duties remains copyright of Great Sankey High School.

Internet materials should contain due copyright acknowledgements for any third party materials contained within them.

Students and staff will be made aware of the implications of infringing, in its various forms, copyright.

Students and staff will not be permitted to use school ICT equipment to access file sharing web sites, copy copyright music or film material.

6. REVIEW

This E-Safety policy is subject to review by staff and governors in the light of developing risks and experience.

Signed...... Date.....

Chair of Governors