Emerson Park School

E-Safety

**Policy to support effective practice
and
Embed Internet Safety**

Contents

Introduction

This e-safety policy should be read in conjunction with:

- EPS Acceptable Use Policy,
- AUP for staff,
- Data Security Policy,
- Child Protection Policy,
- Behaviour Policy and
- Anti-bullying Policy

Roles & responsibilities for internet safety

1. Responsibilities of the Headteacher

- Ultimate responsibility for internet safety issues
- Delegating day-to-day responsibility to a member of SLT as *internet safety co-ordinator*
- Secures time, support and authority for *internet safety team* to function
- Secures funding for technical infrastructure and inset
- Supports the *internet safety co-ordinator*
- Keeps governing body informed

2. Responsibilities of Governors

- Develop an awareness of the issues and risks of using ICT in schools
- Develop an awareness of the benefits of using ICT in schools
- Include internet safety as part of the regular review of child protection and H&S policies
- Develop an understanding of existing procedures and policies for maintaining a safe ICT learning environment
- Support the head teacher in formulating a plan/strategy to deal with media should a serious incident occur
- Promote internet safety to parents

3. Responsibilities of the internet safety co-ordinator

- Establish and maintain a safe ICT learning environment within the school
- Assemble a school *internet safety policy team* to review and advise on internet safety policies
- Work with the internet safety team and head teacher to develop and review appropriate internet safety policies and procedures
- Lead on the development of management protocols so that incidents are responded to in an appropriate and consistent manner
- Lead in the creation of a staff professional development programme that addresses both the benefits and the risks of communication technologies
- Lead in the creation of an internet safety education programme for students
- Maintain an overview of internet safety activities across the school and support different departments
- Develop a parental awareness programme
- Maintain a log of all incidents relating to internet safety in school

- Make recommendations for review of policy
- Meet regularly with the head teacher to discuss internet safety issues and review progress
- Update the governing body on current internet safety issues
- Liaise with outside agencies as appropriate

4. Network Manager & ICT Co-ordinator

- Key members of school internet safety team
- Support internet safety co-ordinator
- Provide and maintain technical infrastructure and information on newly available technologies
- Report network breaches of acceptable use to internet safety co-ordinator

5. Subject Leaders and Heads of Faculty

- Ensure students are properly supervised in ICT suites
- Ensure a co-ordinated approach to teaching and imbedding internet safety
- Discuss general compliance, safety issues and good practise at departmental meetings
- Be familiar with protocols and procedures related to reporting and dealing with breaches in internet safety

6. Heads of House

- Contribution essential in developing a safe ICT learning environment
- Internet safety a big part of ensuring social welfare of students in each house
- Key points of contact in dealing with incidents of ICT misuse/abuse
- Key points of contact for internet safety team
- Impose sanctions within whole-school disciplinary framework
- Supports internet safety co-ordinator in maintaining/developing policies and procedures
- Develop/maintain knowledge of internet safety issues and how it affects children
- Together with internet safety co-ordinator and child protection liaison officer, appropriately support students who experience problems when using the internet
- Act as mediators for ICT related incidents which occur outside school such as bullying within chat rooms, creation of hate websites, etc

7. Classroom teachers and LSA's

- Responsible for internet safety education in the classroom because of increased use of web-based resources and VLE across the curriculum
- Embed internet safety within classroom practise
- Frequently review safety messages
- Acknowledge that internet safety should be recognised in the same way as safety rules in Science laboratories and DT workshops
- Develop and maintain a high level of internet safety awareness

8. SENCO

- Carefully consider the needs of students for whom they have responsibility and whether or not the internet safety programme is appropriate or not, for example a student with autistic spectrum disorder will take messages very literally and could be persuaded to act upon them. Such a student is likely to need additional advice on safe behaviours and what he/she should never disclose to others
- Develop/maintain knowledge of internet safety issues and how it affects children
- Liaise with parents of students with special educational needs to ensure they are aware of the internet safety issues there children may encounter outside school
- Co-operate with child protection liaison officer as necessary

9. CPLO

- Seek professional development on the safety issues related to the use of the internet and related technologies and how it relates to children
- Act as a key member of the internet safety team
- Take a proactive role in the internet safety education of students
- Develop systems for supporting/referring on students referred to them as a result of breaches of internet safety in school
- Develop systems and procedures for students who self-refer and suspected victims
- Develop and maintain strategic partnerships at LEA and external agency level

10. LRC Managers/Librarian

- Key member of the school internet safety team
- Develop and maintain an AUP for the LRC as appropriate to the needs of the school
- Seek professional development opportunities for developing and maintaining knowledge on internet safety issues and how it relates to children and young people

11. Students

- Uphold policies related to acceptable use of the internet and communication technologies
- Develop safe and discriminating behaviours to guide them online
- Report any incident of ICT misuse, abuse and bullying
- Seek immediate help and advice if/when they experience problems when online
- Communicate with their parents/carers about internet safety issues and upholding all the rules for safe internet use at home

Key Stakeholders at Emerson Park School

- Head Teacher & Governors
- Internet safety co-ordinator
- Senior leaders
- Heads of House
- ICT Co-ordinator
- Network Manager
- Subject leaders & Heads of Faculty
- SENCO
- Child Protection Liaison Officer
- Classroom teachers and LSA's
- LRC Manager/Librarian
- Students
- Parents

Putting our Internet Safety Policy into practice

Use of digital and video images

<u>Denveloping a safe school website & the general use of still and moving images</u>

The school website is an important, public-facing communication channel. Many prospective and existing parents find it convenient to look at the school's website for information and it can be an effective way to share the school's good practice and promote its work.

- The ICT Coordinator and/or Web Master will oversee and authorise the school website's content and check suitability. Only the Headteacher, ICT Coordinator and Web Master have the authority to upload content into sections of our website.

- The Web Master will ensure that the school is not infringing on copyright or intellectual property rights through any content published on the website.

- If the school's website contains any guestbook, notice board or blog, they will be monitored by the Web Master to ensure they do not contain personal details of staff or students.

- Links to any external websites will be thoroughly checked by the Web Master before inclusion on our school website to ensure that the content is appropriate both to the school and for the intended audience.

- The school will take care when using photographs or video footage of students on the school website. Group photographs rather than photos of individual children will be taken where appropriate.

- To reduce the risk of inappropriate, unsolicited attention from people outside the school, names of individuals will never be used in photographs.

- Before any photographs of students are published in any form, staff have to adhere to the following two rules:

  - If the student is named, avoid using their photograph / video footage.
  - If the photograph /video is used, do not name the student.

- Whenever the school website is using a webcam it will be checked and monitored by the ICT Coordinator and/or the Web Master to ensure misuse does not occur accidentally or otherwise.

- When showcasing school-made digital video work staff must take care to ensure that students aren't referred to by name on the video and that students' full names aren't given in credits at the end of the film.

- If showcasing examples of students work staff must use only their first names, rather than their full names.

- Only use images of students in suitable dress to reduce the risk of inappropriate use.

- Staff should not to use their personal phone or camera without permission e.g. for a school field trip. If personal equipment is being used it should be registered with the *Internet Safety Coordinator* and a undertaking have to be signed that photographs will be transferred to the school network and will not be stored at home or on memory sticks and used for any other purpose than for school approved business.

Data Protection

- In many cases, it is unlikely that the Data Protection Act will apply to the taking of images e.g. photographs taken for personal use, such as those taken by parents or grandparents at a school play or sports day. However, photographs taken for official school use, which are likely to be stored electronically alongside other personal data, may be covered by the Data Protection Act. As such, students and parents should be advised why they are being taken.

- Parental permission should be obtained before publishing any photographs, video footage etc of students on the school website, in a DVD or in any other high profile public printed media. This ensures that parents are aware of the way the image of their child is representing the school; a printed copy of the specific image should be attached to this form.

Cyber Bullying and Happy Slapping

- Digital images, photographs and video clips can now readily be taken using mobile phones. Extreme abuse is the so called 'happy slapping' incidents sent to others or posted onto a website like YouTube. It is therefore important to ensure that the risk of inappropriate use is minimised.

- For this reason camera/video phones are not allowed in school. All phones brought to school by students have to be handed in at the main reception at the beginning of each day where these will be securely labelled and locked away. Students can collect these phones again after school.

- Incidents of Cyber Bullying via the Internet, School e-mail, mobile communication devices or any other form of digital collaboration/communication technology will be dealt with by the school in strict accordance with the EPS anti-bullying Policy. All such incidents will also be referred to the ISC to evaluate and review e-safety procedures and protocols.

Technical considerations

- Digital images / video of students must be stored securely on the school network and old images deleted after a reasonable period, or when the student has left the school. The ISC will, in conjunction with the Network Manager, monitor this.

- When saving pictures, staff must ensure that the image file is appropriately named. Do not use students' names in image file names or in <ALT> tag references when published on the web? *[An ALT tag is the HTML text describing a displayed image, used mostly for reasons of accessibility, since the tag can be voiced by screen readers]*

- Staff must not use software to 'rip-out' sections of copyrighted movies without permission. There are safe online environments for publishing, such as the Lgfl portal or our VLE.

Educational Programmes

The ISC will devise, implement, monitor and evaluate an Internet Safety Educational Program for students, teachers, governors and parents. This educational plan will mainly aim to achieve three objectives:

1. Inform these stakeholders about the dangers of the Internet,
2. Educate them on how to stay safe,
3. Inform them of what to do when things go wrong
4. Familiarise them with this policy & procedures and the EPS AUP.

Social Networking and Publishing

- The ISC will devise and implement an annual educational programme to make parents and teachers aware that the Internet has online spaces and social networks which allow individuals to publish unmediated content and that those social networking sites can connect people with similar or even quite different interests and that guests can be invited to view personal spaces and leave comments, over which there may be limited control.

- The education program will inform students, parents and teachers of the dangers and advantages of online collaboration and signpost procedures they can follow when things go wrong. Teachers will be reminded about their responsibilities under this policy and what procedures to follow when things go wrong.

- This program will also educate parents and teachers that for use by responsible adults, social networking sites provide easy to use, free facilities; although often advertising intrudes and may be dubious in content.

- The ISC will devise and implement an education program for students that will encourage them to think about the ease of uploading personal information and the impossibility of removing an inappropriate photo or address once published and also inform them about the dangers of collaborating digitally and what to do and who to go to when things go wrong, both in school and out of school.

The Curriculum

As part of the education program for Internet Safety and to further embed e-safety principles, discreet lessons on e-safety will be taught in ICT in year 8 and across the age range in Citizenship.

The Internet Safety Team (IST)

The ISC has formed an Internet Safety team that will meet once a term to discuss the following:

- Review the Internet Safety Policy, AUP, Staff AUP and Data Security Policy
- Review and evaluate the Internet Safety educational programs
- Process Policy updates
- Evaluate Internet Safety protocols so that incidents are responded to in an appropriate and consistent manner

The IST at Emerson Park School is:

- Mrs P Webster (ISC)
- Ms J Marsh (Head of House)
- Miss K Potts (Head of House)
- Ms J Egleton (Head of House)
- Mr G Hobson (Head of House)
- Mr C Trauernicht (ICT Coordinator)
- Mrs B Sumbal (Network Manager)
- Mrs G Mills (LRC Manager)

Response to internet safety incidents in school

```
                        ┌─────────────────────┐
                        │   Internet safety   │
                        │       breach        │
                        └─────────────────────┘
              ┌────────────────────┴────────────────────┐
    ┌─────────────────────┐                    ┌─────────────────────┐
    │ Unsuitable material │                    │  Illegal material or │
    │    or content       │                    │ content (or suspected)│
    └─────────────────────┘                    └─────────────────────┘
              │                                           │
    ┌─────────────────────┐                    ┌─────────────────────┐
    │    Report to ISC    │                    │  Report to Head and │
    │                     │                    │       Police        │
    └─────────────────────┘                    └─────────────────────┘
```

If student: review the incident and decide on appropriate course of action, applying sanctions as necessary	If staff: review the incident and decide on appropriate course of action, applying sanctions as necessary

Report to Head and Police

Secure and preserve evidence

Debrief internet safety team

Await police response

Review policies and technical tools with internet safety team

Implement changes

Monitor

If no illegal material or activity is confirmed: revert to school disciplinary procedures for staff and students	If illegal activity material is confirmed: allow police to complete their investigations, seeking advice from the LEA on interim treatment of staff member or