summerhouse

E-Safety Policy

Overview

The Green Paper *Every Child Matters* and the provisions of the Children Act 2012, Working Together to Safeguard Children sets out how organisations and individuals should work together to safeguard and promote the welfare of children.

The 'staying safe' outcome includes aims that children and 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

Much of these aims apply equally to the 'virtual world' that children and young people will encounter whenever they use ICT in its various forms. For example, we know that the internet has been used for grooming children and 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 children and young people have been exposed to inappropriate content when online, which can sometimes lead to their involvement in crime and anti-social behaviour.

Summerhouse ensures that every child in their care is safe, and the same principles should apply to the 'virtual' or digital world as would be applied to the school's physical buildings.

This policy document is drawn up to protect all parties – the students, the staff and the school and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements.

Managing the Internet Safely

The Internet is an essential element in 21st century life for education, business and social interaction. ICT skills and knowledge are vital to access life-long learning and employment; ICT is now seen as a functional, essential life-skill along with English and Maths. All pupils should be taught to use the Internet efficiently and safely, and to develop a responsible and mature approach to accessing and interpreting information.

The Internet provides many benefits to pupils and the professional work of staff through, for example:

- access to world-wide educational resources, including museums and art galleries
- access to experts in many fields for pupils and staff
- educational and cultural exchanges between pupils world-wide
- collaboration between pupils, professionals and across sectors
- access to learning wherever and whenever convenient

The Internet enhances the school's management information and business administration systems through, for example:

- communication systems
- improved access to technical support, including remote management of networks and automatic system updates
- online and real-time ‘remote’ training support
- secure data exchange between local and government bodies

Summerhouse:

- Pupils are supervised at all times, as far as is reasonable and is vigilant in learning areas
- Uses the LGfL filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming and sites of an illegal nature
- Staff preview all sites before use [where not previously viewed and cached] or only use sites accessed from managed ‘safe’ environments such as the Learning Platform
- Is vigilant when conducting ‘raw’ image search with pupils e.g. Google image search;

- Informs users that Internet use is monitored;
- Informs staff and students that they must report any failure of the filtering systems directly to the ICT consultant. Our systems administrators report to LGfL where necessary;
- Blocks all Chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform
- Has blocked pupil access to music download or shopping sites – except those approved for educational purposes
- Requires all pupils (and their parent/carer) to individually sign an e-safety / acceptable use agreement form which is fully explained used as part the admissions pack
- Requires all staff to sign an e-safety / acceptable use agreement form and keeps a copy on file
- Makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse – through staff meetings and teaching programmes
- Makes information on reporting offensive materials, abuse / bullying etc available for pupils, staff and parents
- Immediately refers any material we suspect is illegal to a member of SLT who will alert the appropriate authorities – Police – and the LA

E mail

E-mail is now an essential means of communication for staff at Summerhouse and increasingly for pupils and families. Directed use of regulated e-mail in schools can bring significant educational benefits, increasing the ease of communication within the school community and facilitating local and international school projects.

However, e-mail can provide a means of access to a pupil that bypasses the traditional school physical boundaries. The central question is the degree of responsibility for self-regulation that may be delegated to an individual. Use of freely available, unregulated email within a school is not appropriate.

Summerhouse has an appropriate educational, filtered Internet-based e-mail option.

In the school context, e mail should not be considered private and most schools, and indeed Councils and businesses, reserve the right to monitor e-mail. There is a balance to be achieved between monitoring to maintain the safety of pupils and the preservation of human rights, both of which are covered by recent legislation.

The use of personal e-mail addresses, such as Hotmail are avoided by all staff and appropriate LA or LGfL systems are used for professional purposes.

Staff and pupils need to be made aware of the risks and issues associated with communicating through e-mail and to have strategies to deal with inappropriate e-mails. This is part of the school's E-Safety and anti-bullying education programme. Pupils need to understand appropriate e-mail behaviour.

Summerhouse:

- Do not publish personal e-mail addresses of staff on the school website. We use postholder or office e-mail address
- If one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law we contact the Police
- Accounts are managed effectively, with up to date account details of users
- Messages relating to or in support of illegal activities will be reported to the relevant Authority and Police

Pupils:

- Pupils are taught about the safety and 'etiquette' of using e-mail both in school and more generally (for example personal accounts set-up at home) i.e. CEOP, 'thinkuknow'
  - not to give out their personal e-mail address
  - they must not reveal private details of themselves or others in e mail, such as address, telephone number, etc
  - to 'Stop and Think Before They Click' and not open attachments unless sure the source is safe
  - that they must immediately tell a teacher/responsible adult if they receive an e-mail which makes them feel uncomfortable, is offensive or bullying in nature;
  - not to respond to malicious or threatening messages
  - not to delete malicious of threatening e-mails, but to keep them as evidence of bullying
  - not to arrange to meet anyone they meet through e-mail without having discussed with an adult and taking a responsible adult with them
  - that forwarding 'chain' e-mail letters is not permitted in school
- Pupils sign the school Agreement Form to say they have read and understood the e-safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

Staff:

- Staff use LA e-mail systems for professional purposes

- Staff should use only the school domain e-mail accounts on the school system when communicating on behalf of Summerhouse
- Staff know that e-mail sent to an external organisation must be written carefully, (and may require authorisation), in the same way as a letter written on school headed paper. That it should follow the school 'house-style'
  - the sending of multiple or large attachments should be limited
  - the sending of chain letters is not permitted
  - embedding adverts is not allowed
- All staff sign our school Agreement Form to say they have read and understood the e-safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

Managing Equipment

The computer network is owned by the school and is made available to students to further their education and to staff to enhance their professional activities including teaching, research, administration and management.

The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet or email activity on the network.

Summerhouse:

- Ensures staff read and sign that they have understood the school's e-safety Policy.
- Makes clear that pupils should never be allowed to log-on or use teacher and staff logins – these have far less security restrictions and inappropriate use could damage files or the network
- Makes clear that no one should log on as another user
- Has set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas
- Requires all users to always log off when they have finished working or are leaving the computer unattended
- Where a user finds a logged-on machine, we require them to always log-off and then log-on again as themselves
- Has blocked access to music download or shopping sites – except those approved for educational purposes;
- Makes clear that staff are responsible for ensuring that all equipment that goes home has the anti-virus and spyware software maintained and up-to-date, and the school provides them with a solution to do so
- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used solely to support their professional responsibilities

- Makes clear that staff accessing LA systems do so in accordance with any Corporate policies
- Maintains equipment to ensure Health and Safety is followed
- (e.g. projector filters cleaned / equipment installed and checked by approved Suppliers / LA electrical engineers
- Ensures that access to the school's network resources from remote locations by staff is restricted and access is only through school / LA approved systems
- Does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is restricted and is only through approved systems;
- Ensures that all pupil level data or personal data sent over the Internet is sent within the approved secure system in our LA
- Follows LA advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network
- Reviews the school ICT systems regularly with regard to security

Developing safe school web sites

The school website is an important, public-facing communication channel. Procedures and practice need to ensure website safety. A senior member of staff will oversee / authorise the website's content and check suitability.

Use of still and moving images

Great care is taken when using photographs or video footage of pupils on the school website. The school obtains consent from parents for use of photos or video footage of children. Their first name and last names will not be displayed in the photograph. An easy rule to remember is:

- If the pupil is named, avoid using their photograph / video footage.
- If the photograph /video is used, avoid naming the pupil.

If showcasing school-made digital video work, pupils aren't referred to by name on the video, and pupils' full names aren't given in credits at the end of the film

When showcasing examples of pupils work, only their first names are used rather than their full names.

Only images of pupils in suitable dress are used to reduce the risk of inappropriate use.

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, pupils and students should be advised why they are being taken.

Parental permission is obtained before publishing any photographs, video footage etc of pupils on the school website.

Procedures:

Links to any external websites are thoroughly checked before inclusion on a school website/learning platform to ensure that the content is appropriate both to the school and for the intended audience. Links are checked regularly, not only to ensure that they are still active, but that the content remains suitable.

Text written by pupils is always reviewed before publishing it on the school website. The work must not include the full name of the pupil, or reveal other personal information. Although it may seem obvious, check that pupils' work doesn't contain any statements that could be deemed defamatory.

The school will also ensure they are not infringing copyright or intellectual property rights through any content published on the website. For example, using images sourced through Google, or using a Trademark for which copyright permission has not been sought.

Mobile Phones

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. Identified children bring mobile phones to school this has to be agreed with the Headteacher. They are to be handed in at the office at the beginning of the day and should be collected at the end of the day.

Staff should be advised not to use their personal phone, tablet or camera without permission e.g. for a school field trip. If personal equipment is being used it should be registered with the school and a clear undertaking 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 school approved business.

Summerhouse has one mobile phone that should be used when taking children out of the school grounds outside of regular school hours. The mobiles will be stored in a safe and secure place within the school office.

Digital images/video of pupils need to be stored securely on the school network and old images deleted after a reasonable period, or when the pupil has left the school.

All staff and pupils know to report any inappropriate use of images to the designated person and understand the importance of safe practice. Staff and pupils understand how to consider an external 'audience' when publishing or presenting work.

Summerhouse:

- The Headteacher takes overall editorial responsibility to ensure that the website content is accurate and quality of presentation is maintained
- Uploading of information is restricted to administration officer and other staff members authorised by the Head Teacher
- The school website complies with the school's guidelines for publications
- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status
- The point of contact on the web site is the school address and telephone number. Home information or individual e-mail identities will not be published
- Photographs published on the web do not have full names attached
- We gain parental / carer permission for use of digital photographs or video involving their child as part of the school enrolment form when child joins a school
- Digital images /video of pupils are stored on the network and images are deleted at the end of the year – unless an item is specifically kept for a key school publication
- We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website
- We do not include the full names of pupils in the credits of any published school produced video materials /DVD
- Staff sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones / personal equipment for taking pictures of pupils
- Pupils are taught about how images can be abused in their E-safety education programme

Social networking and personal publishing

Summerhouse:

- The school will block access to social networking sites
- Pupils will be advised never to give out personal details of any kind which may identify them and / or their location.
- Pupils should be advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph which could identify the student or his/her location e.g. house number, street name or school
- Students are advised not to publish specific and detailed private thoughts
- Children are made aware that bullying can take place through social networking especially when a space has been setup without a password and others are invited to see the bully's comments

How will infringements be handled?

Whenever a student or staff member infringes the e-Safety Policy, the final decision on the level of sanction will be at the discretion of the Headteacher and LA.

How will staff and children be informed of these procedures?

- They will be fully explained and included within the school's E-safety / Acceptable Use Policy. All staff will be required to sign the school's E-safety Policy acceptance form;
- Pupils will be taught about responsible and acceptable use and given strategies to deal with incidents so they can develop 'safe behaviours'. Pupils will sign an age appropriate E-safety / acceptable use form;
- The school's e-safety policy will be made available and explained to parents, and parents will sign an acceptance form when their child starts at the school.
- Information on reporting abuse / bullying etc will be made available by the school for pupils,