Clifton Hill School

E-safety policy

Setting

Clifton Hill School is a special school for students aged between 11 – 19 years who have PMLD, SLD, ASD, challenging behaviour and complex health needs.

Rationale

The E-safety Policy is part of the School Development Plan and relates to other policies including those for ICT, bullying and for child protection.

- The E-safety coordinator is the post holder with Threshold Responsibility for ICT.
- Our E-safety Policy has been written by the school, building on best practice and government guidance. It has been agreed by the senior leadership team and approved by governors.
- The E-safety Policy and its implementation will be reviewed annually.

Teaching and learning

Why Internet and digital communications are important

- The Internet is an essential element in 21st century life for education and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
- The school Internet access is provided by Surrey County through the EasyNet contract and includes filtering appropriate to the age of pupils.
- Where appropriate pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use. (Kidsmart rules are posted around the school close to computer stations).

Protection from inappropriate Internet content

- The school will seek to ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.
- Staff will be taught how to report unpleasant Internet content e.g. using the CEOP Report Abuse icon.
- Content filtering technology is in place as part of the Unicorn contract which prevents access to inappropriate websites.
- Pupils will be supported by a member of staff when using the Internet.

Managing Internet Access

Information system security

- School ICT systems security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed with the Local Authority.

E-mail

- Pupils and staff may only use approved e-mail accounts on the school system.
- Staff monitor pupil e-mail and are aware if pupils should receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Staff to pupil email communication must only take place via a school email address or from within the learning platform and will be monitored.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- E-mail from pupils to external bodies is presented and controlled by staff.
- The forwarding of chain emails is not permitted.
- Passwords will be renewed on a regular basis and systems in place force compliance with this issue.

Published content and the school web site

- The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils personal information will not be published.
- The head teacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified. The school will look to seek to use group photographs where possible. Where full-face photos of individual children are used the school will ensure that their identity is not compromised.
- Pupils' full names will be avoided on the Web site or learning platform particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.
- Parents are clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories. Parents sign a permission form if in agreement on joining the school.

Social networking and personal publishing on the school learning platform

- Pupils must not place personal photos on any social network space provided in the school learning platform.

Managing filtering

- The school will work in partnership with Surrey County Council to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils come across unsuitable on-line materials, the site must be reported to the E-safety Coordinator.

- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing videoconferencing

- Videoconferencing will use the educational broadband network to ensure quality of service and security rather than the Internet.
- Videoconferencing will be supervised by staff.

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Community and third-party experts will be used to identify technology which promotes the school vision.
- Mobile phones and associated cameras must not be used..
- The sending of abusive or inappropriate text messages is forbidden.
- Games machines including the Sony Playstation, Microsoft Xbox and others have Internet access which may not include filtering. Care will be taken with their use within the school use.
- Staff will use a school phone where contact with pupils is required.
- The appropriate use of Learning Platforms will be discussed as the technology becomes available within the school.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 see Data protection policy.

Authorising Internet access

- All staff must read and sign that they will the Staff Code of Conduct for ICT before using any school ICT resource.
- The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.
- Access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.
- Parents will be asked to sign and return a consent form.
- Any person not directly employed by the school will be asked to sign an 'acceptable use of school ICT resources' before being allowed to access the Internet from the school site.

Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor SCC can accept liability for the material accessed, or any consequences of Internet access.
- The school will audit ICT use to establish if the E-safety policy is adequate and that the implementation of the E-safety policy is appropriate and effective.

Handling E-safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the head teacher.

- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

Community use of the Internet

- All use of the school Internet connection by community and other organisations shall be in accordance with the school E-safety policy.

Introducing the E-safety policy to pupils

- Appropriate elements of the E-safety policy will be shared with pupils for whom this is appropriate.
- E-safety rules will be posted in all networked rooms.
- Curriculum opportunities to gain awareness of E-safety issues and how best to deal with them will be provided for pupils where appropriate.

Staff and the E-safety policy

- All staff will be given the School E-safety Policy and its importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Enlisting parents' support

- Parents' and carers attention will be drawn to the School E-safety Policy in newsletters, the school brochure and on the school web site.
- The school will ask all new parents to sign a parent/carer consent form and E-safety rules agreement when they register their child with the school and annually thereafter.

-

Review Date : January 14 by Personnel Committee
Next Review: January 16