Cambridge Steiner School

E Safety Policy
May 2019

Reviewed by: Libby Merritt, Nicola Conlin
Reviewed on: May 2019
Next review: May 2020 (if no legal changes beforehand)

Endorsement
Full endorsement is given to this policy by:

Name: Claudia Goodbrand
Position: Cambridge Steiner School Trustee (Designated Safeguarding Trustee)

Signed: 

Date: 15/5/19

This policy applies to everyone- Staff, Trustees, children, parents/carers, visitors and contractors accessing the internet or using technological devices on the premises. The policy is also applicable where staff or individuals have been provided with setting-issued devices for use off-site.

Online safeguarding, known as online safety is an area that is constantly evolving and as such this policy will be reviewed on an annual basis or in response to an online safety incident, whichever is sooner. Children and young people are likely to encounter a range of risks online highlighted as content, contact and conduct within Annex C of Keeping Children Safe in Education 2018.

The primary purpose of this policy is twofold:

- To ensure the requirement to empower the whole school community with the knowledge to stay safe and risk free is met.
- To ensure risks are identified, assessed and mitigated (where possible) in order to reduce any foreseeable harm to students, Staff, parents/carers, users and the wider school community or liability to the school.

Please also see the Students Acceptable Use Policy for those students who use computers within school and the Use of Mobile Phones and Technological Devices Policy.

1. INTERNET USE

1.1 Why is Internet use important?

The rapid developments in electronic communications are having many effects on society. It is important to state what we are trying to achieve in education through ICT and Internet use.

- Internet use is part of the curriculum for children in Classes 6 onwards and is a necessary tool for learning at Cambridge Steiner School.
- The Internet is a part of everyday life for education, business and social interaction.
- The School has a duty to provide students with quality Internet access as part of their learning experience.
- Pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.
- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the School's management functions.

- Internet access is an entitlement for students who show a responsible and mature approach to its use.

1.2 How does Internet use benefit education?

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to equip our young people with the skills to access life-long learning and employment. Benefits of using the Internet in education include:

- Access to worldwide educational resources including museums and art galleries.
- Educational and cultural exchanges between pupils worldwide.
- Vocational, social and leisure use in libraries, clubs and at home.
- Access to experts in many fields for pupils and staff.
- Professional development for staff through access to national developments, educational materials and effective curriculum practice.
- Collaboration across networks of schools, support services and professional associations.
- Improved access to technical support including remote management of networks and automatic system updates.
- Access to learning wherever and whenever convenient.

2. ACCEPTABLE USE

2.1 Cyberbullying

- For more information please read "Preventing and Tackling Bullying: Advice for School Leaders, Staff and Governing Bodies" http://www.education.gov.uk/aboutdfe/advice/f0076899/preventing-and-tackling-bullying
- DfE and Childnet have produced resources and guidance that can be used to give practical advice and guidance on cyberbullying: http://www.digizen.org/cyberbullying
- Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's Prevention of Bullying Policy.
- All incidents of cyberbullying reported to the school will be recorded by the Safeguarding Team and investigated using the Prevention of Bullying Policy.

Sanctions for those involved in Cyberbullying may include:

- The bully will be asked to remove any material deemed to be inappropriate or a service provider may be contacted to remove content if the bully refuses or is unable to delete content.
- Internet access may be suspended at school for the user for a period of time. Other sanctions for pupils and Staff may also be used in accordance with the School's Prevention of Bullying Policy, Positive Behaviour and Discipline Policy or Acceptable Use Policy.
- Parent/carers of pupils will be informed.
- The Police will be contacted if a criminal offence is suspected.

2.2 Pupils

The rules to which pupils must adhere while using the School's ICT resources are set out in the Pupil Acceptable Use Policy.

2.3 Parents/carers

Any data which contains information about pupils or staff of Cambridge Steiner School should only be published with the school's permission.

Parents should make every effort to attend Parent Meetings concerning online safety provided by the school, and keep up to date with information sent out by the Termly Safeguarding Bulletin or published on the school website.

2.4 Staff

- Staff must not interfere with the work of others or the system itself by attempting to circumvent the network or its security systems.
- Staff must not transmit message or prepare files that appear to originate from anyone other than themselves.
- Staff should not attempt to download and install any software/programs.
- Staff must act reasonably. For instance, the downloading of large files during the working day will affect the service that others receive.
- Users must take responsibility for their network use. Staff should remain mindful of their digital footprint and exercise caution in all their use of social media or any other web-based presence they have. This includes written content, videos or photographs and views expressed either directly or by 'liking' certain pages or posts or following certain individuals or groups.
- Passwords for access to the computer system are confidential and must not be revealed to any other persons. Computers should be secured when not working at the desk e.g. enable Lock Computer settings
- All digital communications with students/parents/carers should be on a professional level and only carried out using official school systems.
- Accessing or storage of any kind of offensive material (including pornography) on the computer system is expressly forbidden. Material will be considered offensive if it causes distress to the person who receives or discovers it.
- Setting-issued devices should only be used for work purposes and, if containing sensitive information or photographs of children, should not leave the premises.
- Serious breach of these rules will be considered gross misconduct for which the normal consequence will be summary dismissal.

3 STUDENT, STAFF, PARENT EDUCATION AND TRAINING

3.1 Online safety in the Curriculum

ICT and online resources are increasingly used across the curriculum. We believe it is essential for online safety guidance to be given to the pupils on a regular and meaningful basis. We have an Online Safety Curriculum that begins at compulsory school age and is continually reviewed and developed in line with national recommendations

Curriculum

Early Years – Learning about Internet Safety through discussions with Kindergarten teacher in Sunbeam group and using pedagogical stories.

Classes 1-3 – Bi-annual special assemblies addressing Internet Safety using pedagogical stories, followed by recall and discussion with Class Teachers.

Classes 4 – 8 – Half termly Internet Safety Lessons following our E Safety curriculum. This has been developed using the Education for a Connected World Framework and the Digital Literacy Programme.

In addition, we use opportunities in everyday discussions with pupils and parent/teacher consultations to address specific issues as they arise.

3.2 Online safety skills development for Staff

New staff receive the School's Staff Code of Conduct, Staff Handbook and Online Safety policy as part of their induction.

All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of online safety and know what to do in the event of misuse of technology by any member of the school community.

Our staff receive information and training on online safety issues in the form of INSET training from the Designated Safeguarding Lead.

3.3 Online safety awareness for Parents/Carers

Parents/carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The School will take every opportunity to help parents understand these issues through termly Safeguarding parents' evenings, a termly Safeguarding Bulletin, parents' evenings, our website online safety page and information about national and local online safety campaigns.

Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

• Photographs and video taken at school events
• Their children's personal devices in the School (where this is allowed)

See also Use of Mobile Phones and Technological Devices Policy.

4. EMAILS

Pupils

- Pupils may use email within school as part of a group project or activity. A class email address will be supplied for this purpose.
- Class emails using this address must be carefully monitored by the Class Teacher and pupils should seek permission before using the address.

  See also Pupil Acceptable Use Policy.

Staff

- Staff will only use official school provided email accounts to communicate with professionals and parents/carers. This allows for email content to be monitored and protects staff from the risk of allegations, malicious emails or inappropriate contact with children and their families.
- Staff must not engage in any personal communications with children who they have a professional responsibility for. This also prohibits contact with children who previously attended the setting.
- The sending of emails from any of the School's email accounts is restricted to School use only

- Staff should not use personal email accounts for professional purposes.
- Staff should not participate in any material that is illegal, obscene and defamatory or that is intended to annoy or intimidate another person or persons.
- All emails should stay professional in tone and checked carefully before sending, just as an official letter would be. Care should be taken when forwarding emails from others.

5. DATA STORAGE AND MANAGEMENT

No electronic documents that include children's names or other personal information, or digital images will be transported out of the setting e.g. on memory sticks or personal laptops.

Setting issued devices should not leave the premises unless encrypted. In the case of an outing, all data must be transferred/deleted from the setting's camera/device before leaving the setting.

6. PUBLISHED CONTENT AND THE SCHOOL WEBSITE.

- The contact details on the website should be the school address, email and telephone number. Staff or pupils' personal information must not be published.
- The Resource Coordinator will take overall editorial responsibility for online content published by the School and will ensure that content published is accurate and appropriate.
- The school website will comply with the School's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.

7. INTERNET CONTENT FILTERING

- The School's broadband access will include filtering appropriate to the age and maturity of pupils.
- Breaches of filtering should be reported immediately to the Resource Coordinator.
- If staff or pupils discover unsuitable sites, the URL will be reported to Resource Coordinator or Safeguarding Team who will then record the incident and escalate the concern as appropriate.
- The Resource Coordinator will ensure all filtering checks are up to date and effective.
- Any material that the school believes is illegal will be reported to appropriate agencies such as IWF, Cambridgeshire Police or CEOP.

7.2 Monitoring

No filtering system can guarantee 100% protection against access to unsuitable sites. The School will therefore monitor the activities of users on the school network and on school equipment as indicated in the School Online Safety Policy and the Acceptable Use Agreement. The School Coordination Team will undertake regular monitoring as part of their termly meetings.

The filtering will be reviewed in the response to the evidence provided by the audit logs of the suitability of the current provision.

7.3 Prevent Duty

The internet provides children and young people with access to a wide-range of content, some of which is harmful. Extremists use the internet, including social media, to share their messages. The filtering systems used in our school blocks inappropriate content, including extremist content.

Where staff, students or visitors find unblocked extremist content they must report it to the Designated Safeguarding Lead.

We are aware that children and young people have access to unfiltered internet when using their mobile phones and staff are alert to the need for vigilance when pupils are using their phones. Pupils are not permitted to use mobile phones during school hours.

Please also see Safeguarding and Child Protection Policy/

7.4 Audit/Reporting

Logs of filtering change controls and of filtering incidents may be made available to:

- The Safeguarding Team
- The School Coordination Team
- The Resource Coordinator
- External filtering provider/Local Authority/Police on request

8. AUTHORISING INTERNET ACCESS

- The School will maintain a current record of all staff and pupils who are granted access to the School's electronic communications.
- All staff will read and sign the Staff Acceptable Use Policy and Online Safety Policy before using any school ICT resources.
- Parents will be asked to read the Student Acceptable Use Policy for pupil access and discuss it with their child, where appropriate.
- All visitors to the school site who require access to the school's network or Internet access will be asked to read and sign an Acceptable Use Policy.
- Parents will be informed that students will be provided with supervised Internet access appropriate to their age and ability.

a. Internet Access for pupils

In classes 6-8, pupils will be supervised. Pupils will use age-appropriate search engines and online tools and online activities will be teacher-directed where necessary. This may include the use of a whole class email address. Pupils of this age may access community ICT facilities, such as in a Public Library, under the close supervision of the Class Teacher and in line with the guidelines set out in the Pupil Acceptable Use Policy.

9. SOCIAL MEDIA

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through:

- Ensuring that personal information is not published.
- Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanction

School staff using social media should ensure that they do not:

- Access personal blogs/social networking sites on work premises or use the setting's internet systems or email address for their own use, without prior agreement or in accordance with the setting's policy.

- Disclose any information that is confidential to the setting or any third party or disclose personal data or information about any individual child, colleague or service user, which could be in breach of the Data Protection Act or the GDPR.
- Disclose the name of the setting or allow it to be identified by any details at all. This includes posting photos of children and young people, the premises or events with work colleagues.
- Link their own blogs/personal web pages to the setting's website.
- make defamatory remarks about the setting, colleagues or service users.

Communication with children and young people, by whatever method, should always take place within clear and explicit professional boundaries. Staff should avoid any misinterpretation of their motives or any behaviour that could be construed as grooming.

Staff should exercise care when using dating websites where staff could encounter students.

Staff must not accept 'friend' invitations or become 'friends' with any pupil of the Cambridge Steiner School on any social media platform or communicate with pupils using any social media site. The School acknowledges that staff may wish to make contact with parents over social media. Staff must exercise professional judgement in these circumstances and should not have any contact with students' family members via social media if that contact is likely to constitute a conflict of interest or call into question their objectivity with regard to the children.

Failure to adhere to the rules and guidelines in this policy may be considered misconduct and could lead to disciplinary and/or criminal investigations.

Remember that anything posted online could end up in the public domain to be read by children, parents or even future employers – so be careful what you post and who you post it to. For example, posting explicit pictures of yourself could damage your reputation and that of your profession and organisation. Parents and employers may also question your suitability to care for children.

Setting social media sites

Setting social networking sites containing information about children attending the setting must be "closed" i.e. the users of the site are accepted and monitored by the manager/administrator. No Staff, families or children's personal information will be accessible by users of the site and the manager/administrator will ensure that users' profiles are kept private. The manager/administrator will moderate all postings to the site; they will view and quality assure these before they appear, for example, to ensure they do not reveal personal information.

10. RISK ASSESSMENT

As the quantity and breadth of information available through the Internet continues to grow it is not possible to guard against every undesirable situation. Our school will need to address the fact that it is not possible to completely remove the risk that pupils might access unsuitable materials via the school system.

The School will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. The School cannot accept liability for the material accessed, or any consequences resulting from Internet use.

- The School will audit ICT use at least annually to establish if the Online Safety policy is adequate and that the implementation of the Online Safety policy is appropriate.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches may be reported to Cambridgeshire Police.
- Methods to identify, assess and minimise risks will be reviewed regularly.

11. RESPONDING TO INCIDENTS OF CONCERN

Where there is cause for concern or fear that illegal activity has taken place or is taking place involving the use of computer equipment, the school will determine the level of response necessary for the offence disclosed. The decision to involve Police will be made as soon as possible, after contacting the Resource Coordinator and DSL, if the offence is deemed to be out of the remit of the School to deal with.

- All members of the School community will be informed about the procedure for reporting online safety concerns (such as breaches of filtering, Cyberbullying, illegal content etc).
- The Resource Coordinator will record all reported incidents and actions.
- The DSL will be informed of any online safety incidents involving Child Protection concerns, which will then be escalated appropriately.
- The Resource Coordinator will manage online safety incidents in accordance with the school discipline/behaviour policy where appropriate.
- The Resource Coordinator will inform parents/carers of any incidents of concerns as and when required.
- After any investigations are completed, the Resource Coordinator will debrief, indentify lessons learnt and implement any changes required.
- Where there is cause for concern or fear that illegal activity has taken place or is taking place then the Resource Coordinator will contact the DSL and escalate the concern to the Police.
- If the School is unsure how to proceed with any incidents of concern, advice will be sought from the MASH (Multi Agency Safeguarding Hub). The School will act in accordance with the Safeguarding and Child Protection policy.

12. ROLES AND RESPONSIBILITIES

As online safety is an important aspect of strategic leadership within the School, the SCT have ultimate responsibility to ensure that the policy and practices are embedded and monitored. Overall Online Safety within the School sits with the Designated Safeguarding Lead, in conjunction with the Resource Coordinator and School Coordination Team. All members of the school community have been made aware of who holds these posts. It is the role of the DSL to keep abreast of current issues and guidance through organisations such as, CEOP (Child Exploitation and Online Protection) and Childnet. http://www.childnet.com/

13. BREACHES OF POLICY

a. - Response to a Breach of Policy

- A breach or suspected breach of policy by a School employee, contractor or pupil may result in the temporary or permanent withdrawal of School ICT hardware, software or services from the offending individual.
- Any policy breach is grounds for disciplinary action in accordance with the School Disciplinary Procedure.
- Policy breaches may also lead to criminal or civil proceedings.

b. - Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the Resource Coordinator in the first instance. Additionally, all security breaches, lost/stolen equipment or data, virus notifications, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the Resource Coordinator.

All online safety incidents involving either staff or pupils should be recorded on the online safety incident log by the Resource Coordinator or DSL.

c. - Complaints

Complaints and/or issues relating to online safety should be made to the Resource Coordinator. Incidents should be logged and the School procedure for investigating an online safety incident should be followed.

13.1 Inappropriate Material

All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the Resource Coordinator.

Deliberate access to inappropriate materials by any user will lead to the incident being logged by the Resource Coordinator depending on the seriousness of the offence; investigation by the SCT, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences.

14. INCLUSION

The school endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the schools' online safety policy.

Useful contacts

Education Child Protection Service	ecps.general@cambridgeshire.gov.uk
Early Years Safeguarding Manager	01223 714760
Local Authority Designated Officer (LADO)	01223 727967

OTHER RELATED POLICIES/DOCUMENTS

Anti-Bullying Policy
Staff Code of Conduct
Use of Mobile Phones and Technological Devices Policy
Safeguarding and Child Protection Policy
Pupil Acceptable Use Policy