Policy Number / Ref	SG_06	
Version	1.1	
Reviewed by / Date	LP/LT	22.11.2016
Approved by / Date	Oliver Clark	22.11.2016
Website upload date	Lisa Patrick	22.11.2016
Further Information	SISEF3 Welfare, health and safety of pupils	

RINGWOOD WALDORF SCHOOL
E-SAFETY POLICY AND PROCEDURE

For clarity, the e-Safety Policy uses the following terms unless otherwise stated:

Users
Refers to staff, governing body, school volunteers, students and any other person working in or on behalf of the school, including contractors.

Pupils
Class 8 and up. (In some instances individual class 7 pupils may be granted access).

Parents
Any adult with a legal responsibility for the child/young person outside the school e.g. parent, guardian, carer.

School
Any school business or activity conducted on or off the school site, e.g. visits, conferences, school trips etc.

Wider school community
School Council, parents.

e-Safety Officers
Louise Tiley, Lisa Patrick.

IT Support
Nigel Roberts

Designated Child Protection Officers (DCPO)
Louise Tiley, Carrol Muckersie, Liz Tomkins

At Ringwood Waldorf School we use technology and the Internet across all areas of the curriculum. Online safeguarding, known as e-safety, is an area that is constantly evolving and as such this policy will be reviewed on a six-monthly basis or in response to an e-safety incident, whichever is sooner.

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, users and the wider school community or liability to the school.

This policy is available for anybody to read on the Ringwood Waldorf School website; upon review all members of staff will sign as read and understood both the e-Safety Policy and the Staff Acceptable Use Agreement. The Student Acceptable Use Agreement will need to be signed before a network account is opened for that student. Upon return of the signed agreement and acceptance of the terms and conditions, students will be permitted access to school technology including the Internet.

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 statutory curriculum and is a necessary tool for Ringwood Waldorf School's learning.
- 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"
www.education.gov.uk/aboutdfe/advice/f0076899/preventing-and-tacklingbullying

DfE and Childnet have produced resources and guidance that can be used to give practical advice and guidance on cyberbullying:
www.digizen.org/cyberbullying

Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated.
All incidents of cyberbullying reported to the school will be recorded.

There will be clear procedures in place to investigate incidents or allegations of Cyberbullying:

- Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.
- The school will take steps to identify the bully, where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- Pupils, staff and parents/carers will be required to work with the school to support the approach to cyberbullying and the school's e-Safety ethos.

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 to the schools anti-bullying, behaviour policy or Acceptable Use Agreement.
- Parent/carers of pupils will be informed.

- The Police will be contacted if a criminal offence is suspected.

2.2 Pupils

In relation to ICT the following are the rules by which pupils must adhere while using the school's ICT resources:

- Pupils must not interfere with the work of others or the system itself by attempting to circumvent the network or its security systems.
- Pupils must not transmit any messages or prepare files that appear to originate from anyone other than themselves.
- Pupils should not attempt to download and install any software/programs.
- Pupils must not create, store or send any message internally or externally which is bullying, abusive, humiliating, hostile or intimidating e.g. sexting, or posting unpleasant images using social media platforms such as Snapchat. Pupils will need permission to send messages to large groups of pupils.
- Pupils must compose any e-mail (or other electronic communication) with courtesy and consideration.

2.3 Parents

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

They should make every effort to attend seminars concerning e-safety provided by the school.

2.4 Staff

Staff are expected to set the example by maintaining the standards outlined in the paragraph titled 'pupils'. In addition:

- 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. For Ringwood Waldorf School staff, flouting the Acceptable Use Agreement may be regarded as a reason for dismissal.
- Workstations should be secured against user mistakes and deliberate actions.
- Resident staff with private Wi-Fi provision must ensure there is no opportunity for students to access their wireless network.

3 STUDENT AND STAFF EDUCATION AND TRAINING

3.1 e-Safety in the Curriculum

ICT and online resources are increasingly used across the curriculum. We believe it is essential for e-Safety guidance to be given to the pupils on a regular and

meaningful basis. E-Safety is embedded within our curriculum and we continually look for new opportunities to promote it.

The school has a framework for teaching Internet skills in ICT/PSHE lessons and tutorial sessions. Educating pupils on the dangers of technologies that may be encountered outside school is also done informally when opportunities arise and as part of the ICT curriculum.

Although not granted access to the school network, pupils in classes 6 and 7 have age appropriate e-safety and digital citizenship sessions to promote e-safety. Children below this age are dealt with, as appropriate, in teacher parent discussions.
Pupils are aware of the relevant legislation when using the Internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them.

Pupils are taught about copyright and respecting other people's information, images, etc. through discussion, modelling and activities.

Pupils are aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying. Pupils are also aware of where to seek advice or help if they experience problems when using the Internet and related technologies; i.e. parent/carer, teacher/trusted staff member, or an organisation such as Childline or CEOP report abuse button.

Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the ICT curriculum.

3.2 e-Safety Skills Development for Staff

New staff receive the school's Acceptable Use Agreement and e-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 e-Safety and know what to do in the event of misuse of technology by any member of the school community.

All staff are encouraged to incorporate e-Safety activities and awareness within their curriculum areas.

Our staff receive information and training on e-Safety issues in the form of INSET from the e-Safety Officer or a nominated person.

4 EMAIL

- Pupils may supply personal email addresses which will be stored for school purposes.
- Pupils must immediately tell a designated member of staff if they receive offensive email.
- Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult.

- Staff will only use official school provided email accounts to communicate with pupils and parents/carers.
- Access in school to external personal email accounts may be blocked.
- Excessive social email use can interfere with learning and will be restricted.
- Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper would be.
- The forwarding of chain messages is not permitted.
- Staff should not use personal email accounts during school hours or for professional purposes.

5 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.

Email addresses will be published carefully online, to avoid being harvested for spam (e.g. by replacing '@' with 'AT'.)

School management 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.

6 INTERNET CONTENT FILTERING

- The school's broadband access will include filtering appropriate to the age and maturity of pupils.
- The school will have a clear procedure for reporting breaches of filtering. All members of the school community (all staff and all pupils) will be aware of this procedure.
- If staff or pupils discover unsuitable sites, the URL will be reported to the School e-Safety Coordinator who will then record the incident and escalate the concern as appropriate.
- Changes to the school filtering policy will be risk assessed by staff with educational and technical experience prior to any changes and where appropriate with consent from the College of Teachers.
- The Network Manager will ensure that regular checks are made to ensure that the filtering methods selected are effective. School management will ensure that this duty forms part of the Network Manager job description and appraisal process.
- Any material that the school believes is illegal will be reported to appropriate agencies such as Internet Watch Foundation (IWF), Dorset Police or Child Exploitation and Online Protection Centre (CEOP).
- The school's access strategy will be designed by educators to suit the age and curriculum requirements of the pupils, with advice from IT Support.

7 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 e-Safety Register to confirm that they have read and understood the e-Safety Policy and Staff Acceptable Use Agreement before using any school ICT resources.
- Parents will be asked to read the Student Acceptable Use Agreement for pupil access and discuss it with their child, where appropriate.
- All visitors to the school site who require access to the schools network or Internet access will be asked to read the Acceptable Use Agreement and sign the e-Safety Register.
- Parents will be informed that pupils will be provided with supervised Internet access appropriate to their age and ability.
- When considering access for vulnerable members of the school community (such as with children with special education needs) the school will make decisions based on the specific needs and understanding of the pupil(s).

According to the year group:

- In the Middle School (classes 7 and 8), pupils will be supervised. Pupils will use age-appropriate search engines and online tools and online activities will be teacher-directed where necessary.
- In the Upper School (classes 9 and up), students will apply for Internet access individually by agreeing to comply with the Student Acceptable Use Agreement.

8 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 to establish if the e–Safety Policy is adequate and that the implementation of the e–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 Dorset Police.

- Methods to identify, assess and minimise risks will be reviewed regularly.

9 RESPONDING TO ANY 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 Child Protection Coordinator or e-Safety officer, 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 e-Safety concerns (such as breaches of filtering, Cyberbullying, illegal content etc).
- The e-Safety Officer will record all reported incidents and actions taken in the School e-Safety incident log and other in any relevant areas e.g. Bullying or Child protection log.
- The DSL will be informed of any e-Safety incidents involving Child Protection concerns, which will then be escalated appropriately.
- The school will manage e-Safety incidents in accordance with the school Behaviour Policy & School Rules where appropriate.
- The school will inform parents/carers of any incidents of concerns as and when required.
- After any investigations are completed, the school will debrief, identify 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 school will contact the DSL or e-Safety officer and escalate the concern to the Police.
- If the school is unsure how to proceed with any incidents of concern, then the incident may be escalated to the Area Children's Officer or the County e-Safety Officer.

10 ROLES AND RESPONSIBILITIES

As e-Safety is an important aspect of strategic leadership within the school, the College of Teachers have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named e-Safety Officers in this school are Louise Tiley and Lisa Patrick. All members of the school community have been made aware of who holds this post. It is the role of the e-Safety Officer to keep abreast of current issues and guidance through organisations such as British Educational Communications and Technology Agency, (BECTA), CEOP.

This policy, supported by the school's acceptable use agreements for staff, visitors and pupils, is to protect the interests and safety of the whole school community.

11 BREACHES OF POLICY

11.1 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.

11.2 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 school's IT Support 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 College of Teachers.

All e-Safety incidents involving either staff or pupils should be recorded on the e-Safety incident log by an e-Safety Officers.

11.3 Complaints

Complaints and/or issues relating to e-Safety should be made to the school management. Incidents should be logged and the School procedure for investigating an e-Safety incident should be followed.

11.4 Inappropriate Material

All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the e-Safety Officers.

Deliberate access to inappropriate materials by any user will lead to the incident being logged by the e-Safety Officers, depending on the seriousness of the offence; investigation by the school management, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences.

12 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' e-Safety Policy.