Policy Number / Ref	SG_04	
Version	2.4	
Reviewed by / Date	LT/HM/NR	Jan 2024
Approved by / Date	BoT	Jan 2024
Review Cycle	Annual	

Online Safety Policy

Including Digital Media Devices

1. Aims

Our school aims to keep all children safe within its care, and this extends to providing both parents and children with the necessary information to remain safe in a digital world. Technology is developing rapidly and it is difficult to stay up to date. We therefore encourage a collaborative approach to Online Safety via education of staff, parents and pupils. This policy will be updated annually or in response to an online safety incident.

We aim to have robust processes in place to ensure the online safety of pupils, staff, volunteers and trustees.

Ringwood Waldorf School aims to provide an ICT free environment for pupils from the ages of 3 – 11. This is from Kindergarten through to Class 6. In those years classrooms are not equipped with interactive whiteboards and pupils have no access to computers or tablets. ICT is introduced gradually from Class 7, starting with a weekly technology lesson. Pupils with SEND may have supervised access to assistive ICT in the classroom if it was deemed necessary for a pupil to help them engage with classroom learning.

Although it is our approach that ICT should be avoided in the years growing up, we nonetheless endeavour to educate the children in the risks involved so that when the technology is used, the risks are minimised. Knowledge and awareness through participation with children is the key to protecting them.

We aim to deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technologies.

We aim to establish clear mechanisms to identify and intervene and escalate an incident, where appropriate.

The 4 key categories of risk

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scam

2. Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools (updated Jan 2023)
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education (updated Sept 2021)
- Searching, screening and confiscation (updated Sept 2022)

It also refers to the Prevent Duty, the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

3. Roles and responsibilities

3.1 The Board of Trustees

The Board of Trustees has overall responsibility for monitoring this policy and holding the School Management Team to account for its implementation.

The BoT will coordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

All trustees will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms of acceptable use of the school's ICT systems and the internet (appendix 2)
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with SEND because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable.

3.2 The School Management Team

The SMT is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The Designated Safeguarding Lead

Details of the school's designated safeguarding lead (DSL) and deputies are set out in our child protection and safeguarding policy.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the SMT in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the SMT, ICT Manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line our Child Protection Policy
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyberbullying are logged and dealt with appropriately in line with the school behaviour policy and anti-bullying policy.
- Updating and delivering staff training on online safety (appendix 3 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the SMT.

This list is not intended to be exhaustive.

3.4 The ICT manager

The ICT manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a regular basis

- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy

This list is not intended to be exhaustive.

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 2), and ensuring that pupils follow the school's terms on acceptable use (appendix 1)
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school's behaviour and anti-bullying policies
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it *could* happen here'.

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

- Notify their child's class teacher/guardian, or any member of staff of any concerns or queries regarding this policy
- When their child reaches Class 9, ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendix 1).
- Guide their children in the appropriate uses of electronic media outside of the school environment, keeping an open dialogue with their children, other class parents and teachers.
- Set up parental controls to ensure safer boundaries. See below for details. However, none of these tools are 100% effective, and the best solution to keeping your child safe online is a combination of controls and parental engagement/supervision.

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues?, UK Safer Internet Centre: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues
- Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics
- Parent factsheet, Childnet International: http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf
- Parental Controls Tutorial: www.safeinternet.org.uk/parental-controls

4. Online Safety Education Strategy

At Ringwood Waldorf School we have various avenues for supporting the online safety of the children.

4.1 Building resilience, self-confidence and self-esteem

Children who feel confident and have high self-esteem are less likely to be drawn into situations where they do things they know they shouldn't. They are more likely to trust their own judgements and seek help when things go wrong.

Steiner-Waldorf Education has at its core the aim to encourage children to be free-thinking, resilient individuals. Our ethos underpins our policies and curriculum, and as such we believe are pupils are well placed to adapt to the challenges.

4.2 Parent Education

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents.

Online safety will also be covered during parents' evenings.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Class Teacher/Guardian or DSL.

4.2.1 Introductory Mornings

All parents are invited to an introductory morning before coming to the school. The use of ICT and its effects are always discussed, and the reasons behind our policy discouraging the use of DMDs is explained. (see Section 8 for DMD policy)

4.2.2 Home-School Agreement regarding use of DMDs. All parents are asked to read, complete and sign the Home-School Agreement.

4.2.3 Parents Evenings. Screens and screen access are regular discussion points at parents' evenings. The teachers aim to create a spirit of openness and non-judgement whilst also reiterating the school's stance on limiting screen access and emphasising actual interpersonal relationships. As the children become older and have more access to DMDs, or start to have their own, class teachers encourage Parent groups to have an agreement on how to handle the use of DMDs when children visit their classmates. For example, respecting each other's boundaries, e.g. no films; all DMDs on the side in the kitchen.

4.2.4 External Talks and advice, for instance Police, NSPCC. These can help clarify the risks and explain recent changes or developments in ICT, as it can be hard for parents to keep up to date with the ever-changing technology. These talks can also help clarify legal responsibilities. These talks were not held during the Covid pandemic, but the school will begin re-initiating these in the next academic year.

4.2.5 Internal Talks/Workshops. Led by members of staff for families within specific classes, or across the school, these can be helpful to share the broader principles of Waldorf Education and put the use of Digital Media into a Waldorf context. They are an important part of overall Parent Education about the Waldorf Curriculum and aims, so that parents understand our position on DMDs and work with us to support our aims as well as formulating strategies for managing this at home.

4.3 Direct Pupil Education: Online Safety Curriculum

Please refer to the PSHE Curriculum policy to see in detail how we deliver online safety education.

Pupils will be taught about online safety as part of the curriculum throughout the school. Before pupils have access to the school's ICT systems from Class 7, online safety will generally be taught through storytelling and discussion. As pupils get older, conversations will become more specific.

In **Kindergarten**, pupils will be taught about online safety through storytelling and parental support. Staff will discuss with parents in parent meetings.

- Use ICT safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies
- Use stories with the children e.g. Firefly the Wood-elf.

Pupils in **Classes 1-4** will be taught to:

- Continued online safety storytelling and discussions, e.g. Anna and the Dragon
- Understand what sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)

In **Classes 5 and 6,** pupils will be taught to:

- Understand a range of ways to use ICT safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns

Pupils in **Classes 7-12** have access to the school network, and therefore at greater risk. They will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- Recognise inappropriate content, contact and conduct, and know how to report concerns
- The safe use of social media and the internet will also be covered in other subjects where relevant.
- The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

By the end of Class 12, pupils will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

In addition, during ICT lessons, all screens will be visible to the teacher.

4.4 School devices for pupil use

We have 13 student ipads (including 3 for SEN), and 15 student laptops. The ipads are all controlled by the Network manager, using apple school manager, and lightspeed mdm (mobile device manager). This means the devices are federated, meaning each student has an individual account on those devices. The ipads are shared ipads.

The ICT manager controls the ipads desktop and apps remotely. They are all subject to the schools web contact filter and they are all youtube blocked. These are primarily for classes 7&8, but the Upper School may use them when needed.

Laptops are only for class 9 +. They are all macbooks and chrome books. These are subject to the web content filter but youtube is accessible. They are only used under teacher supervision. The laptops are not controlled by the MDM, subject to annual review. There are also 3 SEN ipads. One for Colin, Louise, and a 'floating' one. These are the same as the shared ipads. There is a SEN student account on these machines, which the SEN teachers use for lower school students who don;t yet have a school email or login.

All ipads and laptops are stored in a secure device charging station. Network manager holds a log of all IT assets, including serial numbers.

Teachers come to the office, or send students with a signed note. Office staff check them out, and ensure they are checked back in.

5. Cyber-bullying

5.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the *RWS Anti-Bullying Policy* and the *RWS Behaviour Policy*.)

Cyber-bullying, along with all other forms of bullying, by and/or of any member of the school community will not be tolerated.

The main points the school will teach children concerning cyber-bullying are:

- Don't respond
- Don't retaliate
- Talk to a trusted adult
- Save the evidence
- Block the bully
- Be polite
- Don't be a bully
- Be a friend, not a bystander

We will teach parents, if they have been made aware of their child being involved in cyber-bullying, to:

- Listen and take the child seriously
- Make sure the child is safe and feels safe
- Don't overreact
- Encourage the child not to retaliate
- Gather the facts and save the evidence
- Get the child to help solve the problem
- Teach self-esteem and resilience
- Encourage the child to reach out to friends

5.2 Preventing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

Class teachers will actively discuss cyber-bullying with pupils in PSHE lessons, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

All staff, trustees and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The school also sends information, via email or the school newsletter on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

DfE and Childnet have produced resources and guidance on cyber bullying: www.digizen.org/cyberbullying

5.2.1 Response to cyber-bullying

All incidents will be recorded.

Students don't use the school's ICT systems until Class 7, and then under supervision and for a limited time for specific work. As such, the School has deemed it a low risk that cyber-bullying will take place from our systems. However, if this were to be the case, the school will take steps to identify the perpetrator. This would include

examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider, if necessary.

The school will follow the processes set out in the school behaviour and anti-bullying policies. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider in consultation with the Safer Schools Team whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

The perpetrator will have their internet access suspended at school, in addition to any sanctions laid out in the behaviour policy.

5.3 Examining electronic devices

Ringwood Waldorf School does not permit students of any age to use their DMDs on site during school hours. If students are found to be in breach of this, their device will be confiscated. In addition, if there is 'good reason' to search the device, school staff have the specific power for this.

Members of SMT can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the DSL
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's cooperation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident to the DSL immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation

- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our behaviour policy

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

6. Acceptable use of the internet in school

All staff and pupils who will be using the school's ICT systems are expected to sign an agreement regarding the acceptable use of the systems and the internet (appendices 1 and 2).

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited and files downloaded to ensure they comply with the above. In addition, during ICT lessons, the teacher will walk around the room to have full view of all pupil's screens.

More information is set out in the acceptable use agreements in appendices 1 and 2.

7. Pupils' Digital Media Devices in school

This section of the policy also applies to students during events outside school hours, school excursions, camps and extra-curricular activities both on site, and off-site, including the Lantern Centre.

DMDs include all mobile phones, laptops, tablets, smartwatches, iPods and any other device capable of:

- connecting to the internet
- and/or connecting to a mobile network
- and/or connecting to Bluetooth or other wireless connection,
- and/or recording images and/or audio,
- and/or storing images and/or audio,
- and/or displaying digital images and/or audio.

Ringwood Waldorf School recognises that communication through DMDs is an accepted part of everyday life, but that such technologies must be used well. Parents/carers may choose to give their children phones in particular, to protect from everyday risks involving personal security and safety. It is recognised that concern about children travelling alone or commuting long distances to school is alleviated by the possession of a DMD.

Those wishing to bring DMDs to school must hand them in to the office each day they are brought in. (Please note exceptions in Classes 11 & 12 below).

7.1 Responsibilities

The School will keep the child's DMD safe upon it being handed in to the office, to its collection at the end of the day.

Parents/carers decide whether their children may bring a DMD into school. Parents must understand the capabilities of the DMD and potential use/misuse of those capabilities. In addition, it is assumed that household insurance will provide the required cover in the event of loss or damage. The school cannot accept any responsibility for loss, damage or costs incurred due to its use.

Pupils must abide by acceptable use.

7.2 Standard Procedure

- Students are not permitted to use DMDs during school time
- DMDs must be handed into the school office at the start of each day, and collected at the end, up to and including Class 10.
- Allowances may be made in exceptional circumstances, upon request of the parent/carer or teacher. Requests will be handled by the SMT on a case by case basis. Applications for exceptions should be made in writing via the school office. (Class 11 and 12 are allowed their phone, see section 8.5)
- Parents are reminded that in cases of emergency, the school office is a vital and appropriate point of contact and will ensure your child is reached quickly and assisted in any relevant way.

- Unauthorised DMDs will be confiscated and parents contacted to collect.
- Any breach may trigger disciplinary action in line with the school behaviour policy.

7.3 Acceptable Use of DMDs

Where exceptions are permitted, the following rules for acceptable use apply:

- DMDs must not be used without the express permission of the owner.
- DMDs must not be used in any manner or place that is disruptive to the normal routine of the school
- The use of a personal DMD in one lesson for a specific purpose does not mean blanket usage is acceptable. Likewise, permission granted to one student does not mean permission granted to all students in the class, as learning support needs may be a factor.
- Permission may be revoked at any time, and must be returned to the school office at the end of the permitted lesson for safekeeping.
- Bluetooth and other file sharing functions must be switched off at all times.
- DMDs must not be used to exchange images or files
- DMDs must not be used to bully or threaten. It is forbidden for students to use their DMDs to take videos or pictures of denigrating or humiliating acts. This includes photographing or filming any student or member of staff without their consent.
- DMDs must not be taken into changing rooms or toilets, or used in any way that may cause embarrassment or discomfort to their fellow students, staff or visitors to the school.

7.4 Theft and damage

- DMDs should be clearly named
- To reduce the risk of theft, those permitted to have a DMD are advised to keep them concealed
- It is advised that students use passwords/pins to ensure that unauthorised phone calls or messages cannot be made on their DMDs (e.g. by other students, or if stolen).
- DMDs that are found in school must be handed into the school Office
- The school accepted no responsibility for lost, stolen or damaged DMDs, on school site, or travelling from/to school site.

7.5 Class 11 & 12 Exemptions

(This section is taken from the Upper School document: Classes 11 & 12 Technology Use Agreement)

As new technologies continue to change the world in which we live, they also provide many new and positive educational benefits. To encourage this growth, classes 11 and 12 may now bring their own technology to school.

- Only the internet gateway provided by RWS may be accessed while at school.
- Responsibility to keep the device secure rests with the individual owner. RWS, nor its staff or employees, are liable for any device stolen or damaged at school.

The use of technology to provide educational material is not a necessity but a privilege. When abused, privileges will be taken away. When respected, they will benefit the learning environment as a whole. Students and parents/guardians participating must adhere to RWS policies and any Internet Safety guidance.

Additionally, technology:

- May not be used to cheat on assignments or tests.
- May only be used to access files on computer or internet sites which are relevant to the classroom curriculum.
- Games are not permitted.

Students acknowledge that:

- Usage of technology at RWS falls under all the conditions cited in school policies.

- The school's network filters will be applied to all connections to the internet and attempts will not be made to bypass them.
- Bringing on to the premises or infecting the network with a Virus, Trojan, or program designed to damage, alter, destroy, or provide access to unauthorised data or information is in violation of RWS's ICT policy.
- Processing or accessing the information on school property related to "hacking", altering, or bypassing network security policies are in violation of RWS's ICT policy.
- The school has the right to collect and examine any device that is suspected of causing problems or was the source of an attack or virus infection.
- Files may have to be saved to 'cloud' storage (for example Google Drive), the hard- drive, a USB drive, an external drive, or other media device.
- Printing from personal laptops/devices will not be possible at school.
- Personal technology should be charged prior to bringing it to school and should run off its own battery while at school.

8. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date by always installing the latest updates

Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 3.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the ICT Manager

9. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in the behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

10. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation. This will be done through use of and Educare course.

All staff members will receive refresher training at least once each academic year as part of safeguarding training at the pre-term meetings, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings). In addition, Educare courses will be refreshed every two years.

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
    - Abusive, harassing, and misogynistic messages
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
    - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Trustees will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

11. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety through *My Concern*.

This policy will be reviewed annually by the DSL. At every review, the policy will be shared with the board of Trustees.

12. Links with other policies

This online safety policy is linked to the following RWS policies and documents:

- Child protection and Safeguarding policy
- Behaviour Management policy
- Kindergarten Provision Policy
- PSHE Curriculum policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- Staff Code of Conduct

Appendix 1: acceptable use agreement (pupils and parents/carers)

Acceptable use of the school's ICT systems and internet: agreement for pupils and parents/carers	
Name of pupil:	
When using the school's ICT systems and accessing the internet in school **I Promise** – to only use the school ICT facilities for schoolwork that the teacher has asked me to do **I Promise** – not to look for or show other people things that may be upsetting **I Promise** – to show respect for the work that other people have done **I will not** – use other people's work or pictures without permission to do so **I will not** – damage the ICT equipment. I will report any accidents to my teacher immediately. **I will not** – attempt to download and install any software/programs **I will not** – attempt to circumvent the network or its security systems **I will not** – attempt to access any inappropriate websites, or chat rooms **I will not** – attempt to access social networking sites (unless part of a learning activity instructed by teacher) **I will not** – share my password with others or log in to the school's network using someone else's details **I will not** – give my personal information (including my name, address or telephone number) to anyone **I will** – immediately let a teacher know if I find any material which might upset, distress or harm me or others. **I will** – immediately let my teacher know if anybody asks me for personal information or if I find any material which might upset, distress or harm me or others. **I will** – be a good Digital Citizen. I will treat everybody the way that I would like to be treated **I understand** – that some people on the Internet are not who they say they are and that some people can have unpleasant intentions. I will tell my teacher if I am ever concerned in school, or my parents if I am at home. **I understand** – that if I break these rules there will be consequences to my actions and my parents will be told. **If I bring a personal mobile phone or other personal electronic device into school:** **I will** hand it in to the Office at the beginning of the school day, and collect it upon leaving.	
Signed (pupil):	**Date:**
Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 2: acceptable use agreement (staff, trustees, volunteers and visitors)

Acceptable use of the school's ICT systems and the internet: agreement for staff, trustees and volunteers	
Name of staff/trustee/volunteer:	
Internet Access- Staff must not access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature. Inadvertent access must be treated as an online safety incident, reported to the DSL and logged. **Downloads-** Staff must not download large files during the workday, affecting the service others receive. In addition, staff must be aware of download risk regarding viruses and other malware. **Social networking**- Staff must not access social media using the school's systems. In personal time, social networking must never be used to undermine the school, its staff, parents or children. Staff should not become 'friends' with pupils on personal social networks. **Email**- staff are not permitted to use school email addresses for personal business. All email should be professional. Staff are reminded that school data, including emails, is open to Subject Access Requests under the Freedom of Information Act 2000. **Passwords**- These must be kept private. There is no occasion where a password needs to be shared with another member of staff, student or IT support. If you forget your password, please contact the ICT Manager **Images and Videos**- You must not upload onto any internet site or service, any images or videos of yourself, other staff or pupils without consent. This is applicable professionally (in school), and personally (i.e. staff outings) **Personal Use of School ICT**- Staff must not use school equipment for personal use unless specific permission has been given from ICT support who will set the boundaries. **Use of Personal ICT**- Personal equipment in school is used at the discretion of the ICT Manager. Permission must be sought. A risk assessment will be carried out. Staff must abide by the DMD (Staff) Policy.	
I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. I agree that the school will monitor the websites I visit. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will let the designated safeguarding lead (DSL) know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too. I understand that violation of the Acceptable Use agreement may result in dismissal.	
Signed (staff/trustee/volunteer):	**Date:**

Appendix 3: online safety training needs – self-audit for staff

Online safety training needs audit	
Name of staff member/volunteer:	**Date:**
Do you know the name of the person who has lead responsibility for online safety in school?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, trustees and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training? Please record them here.	

Appendix 4: Media and Technology Guidance for Parents and Guardians

MEDIA AND TECHNOLOGY GUIDANCE

At Ringwood Waldorf School we aim to provide our students with opportunities to engage creatively and responsibly with digital technology. In the Waldorf Schools movement we believe that in order for this to happen, children need to be introduced to these technologies gradually and at an appropriate age. We recognise that in order for our students to develop healthy robust bodies, balanced and well-integrated brains, confidence in their real-world practical skills, and strong executive-function capabilities, it is imperative that students primarily interact with one another and their teachers, and work with real materials as much as possible. Our school intentionally develops students and their personal capacity for agency by exploring the world of ideas, participating in the arts, music, movement and practical activities. Their understanding and mastery of technology develops from a solid foundation of hands-on activity and problem solving.

The role of digital technology is central in modern life, and growing research indicates that too much screen time is fundamentally affecting our children. Many of those effects are adverse, no matter how good or educational the content of the programme. Teachers observe that excessive exposure to television, mobile phones and other electronic media significantly shortens the attention span of pupils, stifles the imagination and reduces initiative, patience and perseverance. We therefore discourage young children from using mobile phones, watching television and using electronic games and media. We also strongly recommend that social networking sites are completely out of bounds for younger children and that no child, of any age, is exposed to electronic media in the morning before school or in the hour preceding bedtime as it negatively affects the quality of sleep. Electronic media devices should be kept away from the bedroom and not used alone, and instead used in a shared area of the home.

Electronic media use exposes children to the coercive use of advertising. When exposed too young, the child is unable to discern for themselves what is driving their feeling of need. There is a safeguarding risk in children accessing online games, chat rooms and communication via social media and messaging apps (TikTok, WhatsApp, Snapchat etc), many of which are rated age 16+. Everyone who works with or cares for children has an obligation to keep them safe. Children are not fully equipped to navigate this world of technology at a young age. They are vulnerable to cyber bullying, grooming and seeing inappropriate content which once seen cannot be unseen. In addition, the restricted interaction between a child and a screen, where a child is passively consuming content and not co-creating their reality, can undermine the child’s own creativity. Computer games can be particularly habit-forming and draw the child away from real life experiences. In the context of the Waldorf curriculum, which works so strongly in the child’s imaginative realm, the exposure to television and other electronic media is particularly counter-productive and works against the child’s education.

We recognise that, whilst at home, a child's exposure to electronic and other media lies in the domain of the family. It is therefore parents and carers who must decide what role television and other media play in your children’s lives. However, if the child’s teacher or guardian considers that media use is significantly undermining the healthy development of the child, or the class, this will be brought to the attention of the parents or carers of the children concerned for discussion. Parents and carers should speak to their child’s class teacher, kindergarten teacher, or class guardian - either privately or in parents evenings - about their questions and challenges related to media, so that together we can work out viable approaches. It is very much the wish of the school that parents who bring their children to our Waldorf School will understand and support the school's policy on media and technology.

Further to this, please also be aware that RWS is a Mobile Free Zone for parents, carers, and teachers as well as pupils. Please refer to our *Digital Media Devices (Staff, Volunteers and Visitors) Policy.*

Early Years

Children enrolled in the Kindergarten at Ringwood Waldorf School should be given the gift of a media-free childhood. Kindergarten children should not watch television programmes or films, play video games, or use electronic devices. Additionally, exposure to radio, audiobooks and recorded music should be limited and age appropriate. We encourage parents to keep an open and honest dialogue with their child's kindergarten teacher about their individual circumstances, and teachers are available and willing to assist with reducing screen time and transitioning to a media-free environment in a manageable way.

Lower and Middle School - Class 1 to Class 8

The experience of electronic media can have negative effects on children's learning and development in the Lower School to Middle School. It can also have a detrimental effect on the class dynamic creating a 'those who do and those who do not' situation. Children bring their media experiences into the classroom where it can be quite overwhelming for others. Therefore we ask that access to screens and digital technology is avoided.

Activity on social networking sites and apps should be avoided as children may well become exposed to inappropriate material. It should also be noted that teachers are not permitted to be 'friends' with students on social networking sites nor be in contact through messaging services.

We understand that in some situations it can be difficult to avoid access to screens and digital technology. We propose the following suggestions for managing the children's use of television, games and other electronic media.

1. Access to electronic media should be avoided.
2. Arrange viewing limits, including what can be watched and for how long.
3. Parents/carers should, if possible, watch with the children.
4. Avoid screens in the child's bedroom.
5. Avoid use of portable digital devices (mobile phones, ipads) particularly with access to social networking and video sites e.g. WhatsApp, YouTube, TikTok etc.
6. The telling or reading of bedtime stories is a good way of preparing children for a healthy night's sleep, with no screen use in the hour before bedtime.

As children grow older, television and other media may play a gradually increasing, but hopefully modest part in their lives. It is therefore important to practise regulation with regard to the exposure of young people's minds and senses to modern visual and electronic culture. We suggest that the use of electronic media should be agreed beforehand and take place in the company of family and friends, and not in their own room.

Upper School

RWS has a separate *Digital Media Devices in School Policy* within the *Online Safety Policy* for Classes 8-12 which clarifies in specific detail how, what, where and when DMDs can be used at school.

RWS recognises that teenagers are eager to embrace the modernity of the world they will step into as adults. Our aim is to help them to develop the skills and understanding that provide for mature and discerning use of the new technologies. A familiarity with all the technologies that surround us and influence our lives is an essential part of a complete education. In the Upper School curriculum, Waldorf

education embraces technology in ways that enhance the learning process, by using it as a tool, rather than replace the role of the teacher, and pupils quickly master the technology.