Elmfield Rudolf Steiner School

Media, Computing, Phone and Electronics Policy and Acceptable Use Agreement

November 2019

Policy Tracker – Responsibility for monitoring this policy: **Simon Birch (Interim School Lead)** (Reviewed annually or in response to changes in legislation)			
Date	**Reviewed and Updated By:**	**Role**	**Date Approved by the Governing Board**
16/07/18	Elaine Sheppard	Chair of College	
30/04/19	Elaine Sheppard and Lesley Taberer	Chair of College and Bursar	
11/11/19	Ruth Beachim-Ratcliffe	Designated Safeguarding Lead	**26/11/19**
15/7/20	Name change update		

Statement

At Elmfield we aim to provide our students with opportunities to engage creatively and responsibly with electronic technology. In the Steiner 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 therefore discourage parents from allowing young children to use mobile phones, watching television and DVDs 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.

Though much heated public debate currently surrounds these technologies, there are some very sound reasons for believing that exposure to electronic media fundamentally affects our children. Most of those effects are generally adverse, no matter how good or educational the content of the programme. Some studies have shown, and teachers observe, that exposure to television and other electronic media significantly shortens the attention span of pupils, stifles the imagination, reduces initiative, patience, perseverance, and affects sleep.

Television, cinema and computers also expose children to the coercive use of advertising. In addition, the restricted interaction between a child and a screen genuinely undermines the child's own creativity. In the context of the Waldorf curriculum, which works so strongly in the child's imaginative realm, exposure to television and other electronic media is particularly counter-productive. Computer games can be particularly habit-forming and can break down a child's view of life into cartoon characters. The House of Commons Science and Technology Committee report on '*Impact of social media and screen-use on young people's health*' (2019) outlines benefits, risks and harms following research and investigation.

However, 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 who must decide what role television and other media play in their children's lives. However, if the class teacher or guardian considers that media use is significantly undermining the healthy development of the child or class, this will be brought to the attention of the parents of the children concerned for discussion.

It is very important that parents who bring their children to our school understand and support the school's policy on Media, Computing, Phones and Electronics.

Further to this, please also be aware that Elmfield is a Mobile Free Zone for parents and teachers as well as pupils. We ask you not to use your phone within the school. Staff and pupils are not to use phones unless permission is granted or is a necessity as part of their role.

GUIDING PRINCIPLES:

The school is committed to safeguarding and promoting the welfare of its pupils both within the school environment and outside whilst in the care of the school and this policy intends to give direction as to how the school seeks to educate pupils to use this technology wisely and safely.

The Council of Management have overall responsibility for safeguarding and promoting pupil welfare but is also the responsibility of all staff.

This policy applies to all members of the community when they are on site and also off the school site, but on school business.

The school will adhere to the principles of the General Data Protection Act and other relevant legislation.

This policy should be read in conjunction with other related policies listed in the section entitled application of this policy.

Early Years

In the Early Years, young children can live very strongly into the fairy tale imaginations that they create for themselves from the spoken word. Visual images on a screen allow less scope for this creative inner picturing. Many of the images on screens may also be inappropriate. In the Early Years, children are very good imitators and they may act out things they have seen on the screen, even things that they can barely understand. This can lead to inappropriate play activities.

Lower and Middle School

The experience of electronic media is also unhelpful for children in the Lower School. However, it is understandable that in some families with older siblings some access to electronic media is unavoidable. However, we ask that before 12 years of age access to electronic media should be avoided during the school week. If this is difficult, we propose the following suggestions for managing the children's consumption of television and other electronic media.

1. Arrange viewing limits, including what can be watched and for how long.
2. The parents should, if possible, watch with the children.
3. The telling or reading of bedtime stories is a good way of preparing the children for a healthy night's sleep.

We also recommend that activity on Social Networking sites, in particular, is not allowed at this age.

Middle to Upper School

As children grow older, from the middle school years, television and other media may play a gradually increasing, but hopefully a modest part in their lives. It is therefore important to practise discrimination with regards 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.

Activity on Social Networking Sites should be introduced carefully, with limited and supervised at all times, as youngsters may well become exposed to misuse. Staff are not permitted to be 'Friends' with pupils on Social Networking sites nor be in contact with students via either mobile phones or the internet.

Upper School

Elmfield 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 a mature and discriminative use of the new technologies. For this reason, we have a number of rules within school and guidelines for home.

COMPUTERS: The school aims to train students to be familiar with formatting documents in word processing, creating spreadsheets, setting up PowerPoint presentations and use of databases.

In addition, teachers may show subject-relevant films or clips. Students may be given options as to how to present Main Lesson or GCSE work, and these may well include computer generated components. Teachers may also ask students to research topics online for homework.

STUDENTS WITH SPECIAL EDUCATIONAL NEEDS: The Learning Support department at times recommends that certain students use laptops to take notes and write during lessons. In such cases, parents are requested to ensure the student achieves consistency of access to the equipment. Laptops are also used in exams by candidates with approved access arrangements.

MOBILE PHONES: We ask that all mobile phones are switched off and kept in bags. At the end of the day students should step outside the gates before using phones. The school can accept no liability for phones lost or stolen under this arrangement. Phones seen in use during the school time or within the school grounds will be confiscated unless they are being used with the express permission of a member of staff.

MUSIC PLAYERS: With the occasional exception of use within the confines of GCSE Music or Dance lessons, the rules for MP3 players are the same as for phones.

GAMING: While the school cannot do more than advise, Class Guardians in some cases may choose to converse with parents or guardians, where a student is spending a great deal of time on computer games and consoles. This has noticeable effects on homework and the quality of academic progress in the Upper School.

SOCIAL MEDIA: Parents are advised that social relationships within school can be severely compromised by comments posted on social networking sites from students' homes. In some cases, this may lead to the school initiating bullying investigations. Parents are therefore requested to maintain supervision of their children's online activities.

WHAT THE SCHOOL WILL DO:

The Council of Management and the school have a set of clear expectations and responsibilities for all users and on behalf of the Council of Management, the Coordination Group (CG) will:

- Maintain and implement a series of policies and procedures through which behaviour and actions can be moderated, risk may be assessed, controlled or mitigated and which will provide the means for acting and reporting on issues thereby securing the welfare of pupils.
- Designate a member of staff to be the Online Safety Officer who may be delegated to act on any matters within this Policy as well as taking day to day responsibility for online safety issues. This is Ruth Beachim-Ratcliffe, who is also the school's Designated Safeguarding Lead (DSL).
- Ensure all staff are: aware of and adhere to the School`s policies and procedures for the health, safety and welfare of pupils; appropriately trained in matters of online safety and are vigilant for any signs of potential misuse; aware of the regulations permitting and guiding the searching of electronic devices.
- Provide adequate and suitable education for pupils through the curriculum so that they can be better informed in the use of, and potential threats/risks associated with the use of the internet and of electronic devices.
- Engage with parents to ensure that they are equally well informed of the risks and dangers.
- Ensure that there is a clear and consistent approach for responding to incidents.
- Liaise and share information about concerns with local and national agencies who need to know and involve pupils and parents appropriately.
- Appraise the Council of Management annually of education and training initiatives undertaken, any identified risks and any incidents. Reporting should be more frequent where incidents are serious or frequent.

PUPILS AND THEIR PARENTS/CARERS:

- Pupils are required to assume responsibility for their behaviour, and this extends to their use of the internet and any other electronic devices.
- Pupils should be respectful and tolerant of others and be mindful of, and responsible for their own welfare and that of others.
- Any form of bullying or harassment will not be tolerated.
- The Education and Inspections Act 2006 permits the regulation of the behaviour of the pupils when they are off the school site including the imposition of sanctions for inappropriate behaviour. This is pertinent to cyber–bullying or other e–safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.
- Pupils should be aware of how they can report areas of concern.

STAFF:

- All staff and volunteers should adhere to this policy and be good role models in their use of the internet and mobile devices.
- Have an understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Any online safety incident is to be brought to the immediate attention of the DSL who will deal with the matter.

ACCEPTABLE USE AGREEMENT:

- Upper school pupils, staff and volunteers are required to sign the School`s Acceptable Use Agreement as appropriate.
- Visitors will be informed of the School`s Acceptable Use Agreement on arrival.
- Use of the School`s internet and devices are intended for school business or professional development.

APPLICATION OF THIS POLICY:

- Technology advances rapidly, however the responsibility to safeguard pupils remains constant and so the School will develop the principles of this policy to a sufficient degree to provide a working document that will set out and explain how the School applies these principles in practice.
- This policy should be read in conjunction with the following policies:

  - ❖ Anti-Bullying Policy
  - ❖ Anti-Radicalisation Policy
  - ❖ Behaviour and Discipline Policy
  - ❖ Staff Code of Conduct Policy
  - ❖ Child Protection Policy: Safeguarding Children
  - ❖ Confidentiality Policy
  - ❖ Data Protection Policy
  - ❖ Mobile Phone Policy
  - ❖ School Trip Behaviour Policy
  - ❖ School Trip Code of Conduct Policy
  - ❖ Staff Code of Conduct

  Guidance:

    - o Working Together to Safeguard Children (July 2018)
    - o Keeping Children Safe in Education (September 2019)

ROLES AND RESPONSIBILITIES:

- Online safety is an important aspect of strategic leadership within the school and the CG and Council of Management have ultimate responsibility to ensure that the policy and practices are embedded and monitored.
- It is the role of the Co-ordination Group to keep abreast of current issues and guidance through organisations such as CEOP, Childnet and others.
- It is the responsibility of all staff to protect and secure the welfare of all pupils.

MONITORING:

- An authorised member of staff may inspect any school ICT equipment at any time without prior notice.
- To the extent permitted in law, authorised staff my access, inspect and disclose telephone calls, e-mails and any other electronic communications involving students, staff or visitors, without consent.
- Authorised staff may access the e-mail where applicable of someone who is absent in order to deal with any business-related issues retained on that account.
- All monitoring or investigative activities are conducted ay authorised staff and comply with GDPR regulation, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000.

BREACH OF POLICY:

- A breach or suspected breach of policy by a staff member, pupil or visitor may result in the temporary or permanent withdrawal of school ICT usage for that individual/individuals.
- Any policy breach is grounds for disciplinary action in accordance with the School`s Behaviour Policy or Disciplinary Procedure as appropriate.
- Policy breaches may also lead to criminal or civil proceedings.
- Any security breaches or attempts, loss of equipment and any unauthorised use of ICT must be immediately reported to the Data Protection Officer in the first instance.
- Complaints and/or issues relating to online safety should be made to the DSL.
- Complaints will be dealt with in accordance with the School`s Complaints Policy or staff Grievance Procedure as appropriate.
- All incidents should be logged and the School`s procedure for investigating incidents and recording complaints should be followed.
- Accidental access to inappropriate materials must be immediately reported to the DSL or their Deputy.
- Deliberate access to inappropriate materials may lead to the incident being directly referred to the DSL and depending on the seriousness of the offence, this may lead to immediate suspension, possibly leading to exclusion/dismissal and, where appropriate, referral to the police for very serious offences.

INCLUSION:

- Pupils may join at different stages with varied and different understandings of online safety. The school endeavours to create a consistent message with pupils and parents which in turn should help, establish, cement and further develop the School`s online safety rules.
- Staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of online safety. Issues.
- Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of online safety.

COMPUTER VIRUSES:

- It is important that staff, volunteers and pupils never interfere with any anti-virus software installed on school ICT equipment.
- Any interference with antivirus software or any absence of antivirus software will be treated as a serious breach of policy.

DATA SECURITY:

In accordance with the General Data Protection Regulation (GDPR) 2019, we ensure that personal information held electronically is:

- held and used with the subject’s knowledge and permission
- held and used for specifically stated purposes only
- kept for no longer than is necessary
- handled according to people’s data protection rights
- kept safe and secure
- shared with or transferred to other bodies in accordance with the school’s Data Protection Policy. Please refer to this policy for further information.

PUPIL AND STAFF EDUCATION TRAINING:

- It is essential that online safety guidance is given to the pupils on a regular basis as it is increasingly used. Online safety is embedded within our curriculum and we continually look for new opportunities to promote online safety.
- 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/teacher/trusted staff member or an organisation such as Childline or CEOP report abuse button.
- Whole school assemblies and tutorials are also to be used to keep current the understanding and importance of online safety.
- New staff receive information on the School`s Media and Acceptable Use policy as part of their induction.
- All staff must be aware of individual responsibilities relating to the safeguarding of pupils 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.
- All staff are encouraged to incorporate online safety activities and awareness within their curriculum areas.
- Information and training updates on online safety issues are provided.
- Staff complete Prevent awareness training in order to become more familiar with the signs and symptoms of extremism and appropriate responses to it.
- Staff have access to Educare online courses including e-safety.

SYSTEMS AND ACCESS:

- All staff are responsible for any activity on school systems carried out under access/account rights assigned to them whether accessed via school ICT equipment or their own PC.
- No member of staff should allow any unauthorised person to use school ICT facilities.
- Staff should use only their personal logons, account IDs and passwords and not allow them to be used by anyone else.
- Staff should ensure they log off before moving away from a computer during the working day to protect any personal, sensitive, confidential or otherwise classified data and to prevent unauthorised access. Staff should also ensure that any sensitive data is secure and not downloaded to any shared areas.
- Staff should not introduce or propagate viruses knowingly.
- It is imperative that staff do not access, load, store, post or send from school ICT any material that is, or may be considered, illegal, offensive, libellous, pornographic, obscene, defamatory, intimidating, misleading or disruptive to the School or may bring the school into disrepute. This includes, but is not limited to, jokes, chain letters, files, emails, clips or images that are not part of the School`s business activities; sexual comments or images, nudity, racial slurs, gender specific comments, or anything that would offend someone on the basis of their age, sexual orientations, religious or political beliefs, national origin, or disability.
- Any information held on school systems may be subject to the Freedom of Information Act.

- Where necessary, obtain permission from the owner or owning authority and pay any relevant fees, before using, copying or distributing any material that is protected under the Copyright, Designs and Patents Act 1998.

ICT EQUIPMENT WITHIN THE SCHOOL:

- Pupils are responsible for their activity on the School`s equipment.
- Users are responsible for ensuring that any information accessed from their own PC, Laptop or removeable media equipment is kept secure, and that no personal, sensitive, confidential or classified information is disclosed to any unauthorised person. All devices should be password protected.
- Equipment must be kept physically secure in accordance with this policy to be covered for insurance purposes including when travelling.
- In areas where there may be members of the general public, portable or mobile ICT equipment must not be left unattended and wherever possible must be kept out of sight.
- Staff are permitted to bring in personal mobile phones and devices for their own use. Under no circumstances is a member of staff permitted to contact a pupil or parent using their personal device unless it is for the purpose of enhancing their duties. (e.g. contacting a student with information during a school trip.)
- Pupils are permitted to bring their own mobile phones in to school but must turn them off and in the lower classes (5 - 8) these are handed in and collected by the class teacher. Upper school pupils are to keep them switched off and kept in their bag, unless they are given permission by a teacher to carry out research in a lesson. This must be supervised by the teacher and is not permitted without the teacher present. If a pupil is found using their phone whilst not on research for school, then their phone will be confiscated and taken to the school office. This will be kept in the safe and logged and three defaults will result in an after-school detention.
- The school is not responsible for the loss, damage or theft of any personal mobile device.
- Permission must be sought before any image or sound recordings are made on these devices of any member of the school community.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

ACCEPTABLE USE:

At Elmfield, we neither promote the use of electronic technologies in the Early Years nor in Lower or Middle school for pedagogical reasons. However, in the Upper School, we do encourage the use of electronic technologies in children's independent study at home and where appropriate in lessons at school. This can be a powerful tool to enhance learning and is seen as one of many research tools which children need to be adept at using. All pupils have an entitlement to safety on line and the school and staff are responsible for ensuring this happens.

This Acceptable Use agreement is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational and personal use.
- that school and staff are protected from potential risk in their use of technology of everyday work.

The school will try to ensure that staff will have appropriate access to digital technology to enhance their work and Upper School pupils will be permitted to use electronic technologies where deemed appropriate to enhance their learning opportunities. In return, pupils and staff are expected to be responsible users.

Staff and Volunteer Acceptable Use Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise that I have a responsibility to guard my personal and the school`s good reputation and any breach of this agreement could bring the school and myself into disrepute. I will ensure that the pupils who are using electronic technologies are always supervised by myself or another staff member directly.

For my professional and personal safety:

- I understand that the school has a responsibility to oversee my use of electronic technology.
- I understand that the rules set out in this agreement also apply to the use of technologies outside of school (e.g. emails, laptops etc) and to the transfer of personal data out of school.
- I will not disclose my password to anyone else and I will not use any other person`s name or password. I will not disclose the password to any pupils to access the electronic technology in the upper school.
- I will immediately report any illegal, inappropriate or harmful material or incident I become aware of to the DSL.

I will be responsible in my communications and actions when using school communications:

- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take or publish images of others I will do so with their permission and in accordance with the school`s policy of the use of digital images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published, it will not be possible to identify by name or other personal information, those who are featured.
- I will only communicate with pupils and parents/carers using official school systems. Any such communication will be professional in tone and manner. Should it be deemed necessary to share personal details such as personal mobile numbers then I am aware of the inherent risks and take responsibility for this. Any communication about school related business and pupils should only be from my school email and not my personal email.
- I will not engage in any on-line activity, including Social Media, that may compromise my professional responsibilities or the reputation of the school.

The school has the responsibility to provide safety for all within the school community and to ensure the smooth running of the school:

- When I use my personal mobile devices, laptops etc, I will follow the rules set out in this agreement. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses and are password protected.
- I will not open any hyperlinks in emails or any attachments to emails, unless source is known and trusted or if I have any concerns about the validity of the email.
- I will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering systems in place to prevent access to such materials.

- I understand that the Data Protection Policy requires that any staff or pupil data to which I have access will be kept private and confidential, except when it is deemed necessary that I am required by law or by school to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or password breaches, however this may have happened.
- I will not download personal or sensitive data to shared computers within the school.

When using the internet in my professional capacity:

- I will ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not download or distribute copies.

Agreement:

I understand that I am responsible for my actions in and out of the school.

- I understand that this Acceptable Use Policy applies not only to my work and use of school digital technology equipment in school but also applies to my use of school systems off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Agreement, I could be subject to a disciplinary action.

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff/volunteer Name:

Signed:

Date:

Related Policies

Anti-Bullying Policy
Anti-Radicalisation Policy
Behaviour and Discipline Policy
Child Protection Policy: Safeguarding Children
Confidentiality Policy
Data Protection Policy
Mobile Phone Policy
School Trips Behaviour Policy
School Trips Code of Conduct
Staff Code of Conduct Policy

Pupil Acceptable Use Agreement (Upper School Only)

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.

For my personal safety:

- I understand that the school has a responsibility to oversee my use of electronic technology.
- I will not disclose or share personal information about myself or others when on-line.
- I will not disclose my password to anyone else and I will not use any other person`s name or password.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line. I know that I should report this to the school's Designated Safeguarding Lead and also to my Class Guardian.

I will be responsible in my communications and actions:

- I will communicate with others in a polite and responsible manner. I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take or publish images of others, I will do so with their permission and in accordance with the school`s policy of the use of digital images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published, it will not be possible to identify and individual by name.
- I will not engage in any on-line activity, including Social Media, that may compromise my personal responsibilities or the reputation of the school.

I understand that the school has the responsibility to maintain the security and integrity of the technology it offers and to ensure the smooth running of the school:

- When I use my personal mobile devices, laptops etc, I will follow the rules set out in this agreement. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software, are free from viruses and are password protected.
- I will not open any hyperlinks in emails or any attachments to emails, unless source is known and trusted, or if I have any concerns about the validity of the email.
- I will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering systems in place to prevent access to such materials.
- I will not use the school IT systems for on-line gaming, on-line gambling, internet shopping, file sharing or video broadcasting
- I understand that the Data Protection Policy requires that any data to which I have access will be kept private and confidential, except when it is deemed necessary that I am required by law or by school to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or password breaches, however this may have happened.
- I will not download personal or sensitive data to shared computers within the school.

When using the internet in my education:

- I will ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not download or distribute copies.
- When I am using the internet to find information, I will take care to check that the information I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.
- I will not view or download inappropriate websites or images, including those defined in this policy.

Agreement:

I understand that I am responsible for my actions in and out of the school:

- I understand that the school has the right to take action against me if I am involved in incidents of inappropriate behaviour that are covered in this agreement, including when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Agreement, I could be subject to a disciplinary action. This may include detentions, exclusion, contact with parents and, in the event of illegal activities, involvement of the police.

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to my education and with the school community) within these guidelines.

Pupil Name:

Signed:

Date:

Related Policies

Anti-Bullying Policy
Anti-Radicalisation Policy
Behaviour and Discipline Policy
Child Protection Policy: Safeguarding Children
Confidentiality Policy
Data Protection Policy
Mobile Phone Policy
School Trips Behaviour Policy
School Trips Code of Conduct
Staff Code of Conduct Policy