Michael Hall
a Steiner Waldorf School

Online Safety Policy

Policy Owner	**Designated Safeguarding Lead**
Policy Lead	**Senior Leadership Team**
Formally endorsed by	**Council of Trustees**
Endorsement Date	**August 2019**
Next Review Date	**August 2020**

POLICY STATEMENT

Online safeguarding, known as online safety is an area that is constantly evolving and as such this policy will be reviewed on an annual basis or in response to an online safety incident, whichever is sooner. Keeping Children Safe in Education 2019 states;

An effective approach to online safety empowers a school or college to protect and educate the whole school or college community in their use of technology and establishes mechanisms to identify, intervene in and escalate any incident where appropriate.

As such this Online safety policy provides us with a framework to develop our online safety ethos and enables leaders and managers to detail strategic approaches and considerations, with regards to the safer use of technology.

The primary purpose of this policy is:

- to safeguard and protect all members of Michael Hall's community online.
- to identify approaches to educate and raise awareness of online safety throughout the community.
- to enable all staff to work safely and responsibly, to role model positive behaviour online and to manage professional standards and practice when using technology.
- Identify clear procedures to use when responding to online safety concerns.

Policy Scope

Michael Hall believes that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all learners and staff are protected from potential harm online.

Michael Hall identifies that the internet and associated devices, such as computers, tablets, mobile phones and games consoles, are an important part of everyday life.

Michael Hall believes that learners should be empowered to build resilience and to develop strategies to manage and respond to risk online.

This policy applies to all staff including the governing body, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the setting (collectively referred to as "staff" in this policy) as well as learners, parents and carers. (Amend staff roles as appropriate to the setting)

This policy applies to all access to the internet and use of technology, including personal devices, or where learners, staff or other individuals have been provided with setting issued devices for use off-site, such as a work laptops, tablets or mobile phones.

This policy is available for anybody to read on the Michael Hall School website; upon review all members of staff will sign as read and understood both the Online Safety Policy and the Staff Acceptable Use Policy (found within the Staff Code of Conduct). The Students Acceptable Use Policy will need to be signed before a network account is opened for that student. Upon return of the signed permission slip and acceptance of the terms and conditions to the Admin Office, students will be permitted access to school technology including the Internet.

Children and young people are likely to encounter a range of risks online highlighted as content, contact and conduct within Annex C of 'Keeping Children Safe in Education' 2019'

1. INTERNET USE.

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 Michael Hall'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 use at school is permitted using school equipment only. This is in order for us to be able to monitor its use and provide our student with a safe environment. Access to the internet using personal devices is not permitted whilst on the school site, please see Mobile Phone Policy.

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.

Cyberbullying.

For more information please read "Preventing and Tackling Bullying: Advice for School Leaders, Staff and Governing Bodies" http://www.education.gov.uk/aboutdfe/advice/f0076899/preventing-and-tackling-bullying

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

Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's Anti-bullying and Behaviour Policies.

All incidents of cyberbullying reported to the school will be recorded by Compliance Officer and reported to the Safeguarding team.

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

- 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 online 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 Policy.
- Parent/carers of pupils will be informed.
- The Police will be contacted if a criminal offence is suspected.

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 should not attempt to access any inappropriate sites
- 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.

Parents

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

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

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 Michael Hall staff, flouting the Acceptable Use policy 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.
- All digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official school systems

3. STUDENT, STAFF AND PARENT / CARERS EDUCATION AND TRAINING

Online safety in the Curriculum.

ICT and online resources are increasingly used across the curriculum. We believe it is essential for online safety guidance to be given to the pupils on a regular and meaningful basis. Online safety is embedded within our curriculum and we continually look for new opportunities to promote it. All Class teachers, Guardians and the Online Safety Officer who are responsible for the delivery of the online safety curriculum have been issued with the Teaching Online Safety in School 2019 Guidance and are aware that that they should refer to the Education for a Connected World Framework for ager specific advice about the knowledge and skills that pupils should have the opportunity to develop.

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 from age 5 will have age appropriate online safety and digital citizenship sessions to promote online safety. This may be met through a variety of

ways including PHSEE and/ or stories. Children below this age are dealt with, as appropriate, in teacher parent discussions.

Older 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.

Through their class teacher or Guardian, students have a safe space to raise concerns and discuss issues that are immediate and relevant to them.

Online Safety Skills Development for Staff.

New staff receive the school's acceptable use policy and Online Safety policy as part of their induction.

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

All staff are encouraged to incorporate online safety activities and awareness within their curriculum areas.

Our staff receive information and training on online safety issues in the form of INSET/online training from the Online Safety Officer or a nominated person.

Online safety awareness for Parents/Carers.

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The School will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, the Michael Hall website online safety page and information about national & local online safety campaigns. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- their children's personal devices in the school (where this is allowed)

A useful resource: http://www.eastsussexlscb.org.uk/our-priorities/online-safety/

4. EMAIL

- Pupils from Y8 upwards are provided with a school email address.
- Pupils must immediately tell a 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 and whenever possible send email communication via iSAMS so that a central record of the communication is stored.
- 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 WEBSITES

The contact details on the website should be the school address, email and telephone number. Staff or pupils' personal information must not be published.

The Senior Leadership Team (SLT) 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 Online Safety Officer who will then record the incident and escalate the concern as appropriate, notifying the Safeguarding Team and keeping them updated.
- 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 SLT.
- The IT Administrator will ensure that regular checks are made to ensure that the filtering methods selected are effective reporting finding to the Online Safety Office and SLT. The Online Safety Officer with agreement from SLT will instruct the IT Administrator of any changes required to the filtering requirements. SLT will ensure this duty forms part of the Online Safety Officer job description and appraisal process.
- Any material that the school believes is illegal will be reported to appropriate agencies such as IWF, Sussex Police or CEOP.

Monitoring

No filtering system can guarantee 100% protection against access to unsuitable sites. The School will therefore monitor the activities of users on the school network and on school equipment using a classroom management system allowing us to monitor student PC usage, browsing history, and app usage.

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

Prevent Duty

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

Where staff, students or visitors find unblocked extremist content they must report it to the Online Safety Officer or the Safeguarding Team.

As a school we do not allow the use of personal devises whilst on the premises, however we are aware that children and young people have access to unfiltered internet when using their mobile phones (via 3G or 4G) and staff are alert to the need for vigilance if they observe pupils using their phones. Any identified incidents will be logged and action determined on a case by case basis.

Audit/Reporting

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

- The Safeguarding Team
- The Senior Leadership Team
- External filtering provider/Local Authority/Police on request

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 Staff Acceptable Use Policy and Online Safety Policy before using any school ICT resources.
- The Student Acceptable Use Policy for pupil access will be issued annually by the Class Teacher/Guardian. Discussion will take place in class to ensure that all students understand the agreement prior to them signing it.
- The Student Agreement will be published on both the Student and Parent Portal for information.
- All visitors to the school are not given access to the school's network, should this be required they will be asked to read and sign an Acceptable Use Policy.
- 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 to 12), students will apply for Internet access individually by agreeing to comply with the School Online Safety Rules or Acceptable Use Policy.

8. SOCIAL MEDIA – PROTECTING PROFESSIONAL IDENTITY

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

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

School staff should ensure that:

- No reference should be made in social media to students / pupils, parents / carers or school staff
- They do not include pupils in their friends, or contact lists
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

9. 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 (360 Degree Safe Tool) to establish if the Online Safety policy is adequate and that the implementation of the Online Safety policy is appropriate.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches may be reported to Sussex Police.
- Methods to identify, assess and minimise risks will be reviewed regularly.

10. 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 Online Safety Officer and DSL, if the offence is deemed to be out of the remit of the school to deal with.

- The Compliance Officer will record all reported incidents and actions taken in the School Online Safety incident log.
- The DSL will be informed of any online safety incidents involving Child Protection concerns, which will then be escalated appropriately.
- The School will manage online safety incidents in accordance with the school discipline/ behaviour policy 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 and escalate the concern to the Police.
- If the School is unsure how to proceed with any incidents of concern, advice will be sought from SPOA. The School will act in accordance with the child protection and safeguarding policy and the relevant Pan Sussex Child Protection and Safeguarding procedures.
- Whilst the use of mobile phones is not encouraged on the school site, we acknowledge that some students may not adhere to the rules. Staff should be vigilant and report inappropriate use of 3G & 4G connectivity by any students that have been found to be using mobile devices.

11. ROLES & RESPONSIBILITIES

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

12. BREACHES OF POLICY

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.

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 Compliance Officer 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 Senior Leadership Team.

All online safety incidents involving either staff or pupils should be recorded in the online safety incident log by the Compliance Officer.

Complaints

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

Inappropriate Material

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

Deliberate access to inappropriate materials by any user will lead to the incident being logged by the Online Safety Officer, depending on the seriousness of the offence; investigation by the Senior Leadership Team, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences.

13. INCLUSION

The school endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the schools' online safety policy. The Policy will be reviewed annually by the Online Safety Officer, Designated Safeguarding Lead, Safeguarding Team, Senior Leadership Team.

Council Chair
Sean Rafferty

For clarity, the Online Safety policy uses the following terms unless otherwise stated:

- Users - refers to staff, trustees, school volunteers, students and any other person working in or on behalf of the school, including contractors.
- Pupils – age 5 and above.
- 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.
- IT Support – An appointed external IT consultancy
- Designated Safeguarding Leads (DSL)
- Deputy Designated Safeguarding Leads (DDSL)