MAHARISHI SCHOOL

Online Safety Policy

March 2023

Start Date: March 2023

Review Date: March 2025

Signed by:

Headteacher	Lisa Edwards	Date	Mar 23
Chair of Governors	Ian Birnbaum	Date	Mar 23

Contents:

Statement of intent

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 information and business administration systems. The internet is an essential element of 21st Century life; in education, business and social interactions. Maharishi School is committed to providing pupils with quality internet access as part of their learning experience.

The purpose of this policy is to:

- establish rules for using the internet and electronic equipment in school
- establish how these fit into the wider context of our Enabling Good Behaviour Policy and PSHE policy.
- demonstrate the methods used to protect pupils from unsuitable material

1. Legal framework

This policy has due regard to all relevant legislation and statutory guidance including, but not limited to, the following:

Voyeurism (Offences) Act 2019

The UK General Data Protection Regulation (UK GDPR)

Data Protection Act 2018

DfE (2021) 'Harmful online challenges and online hoaxes'

DfE (2022) 'Keeping children safe in education 2022'

DfE (2023) 'Teaching online safety in school'

DfE (2022) 'Searching, screening and confiscation'

Department for Digital, Culture, Media and Sport and UK Council for Internet Safety (2020) 'Sharing nudes and semi-nudes: advice for education settings working with children and young people'

UK Council for Child Internet Safety (2020) 'Education for a Connected World – 2020 edition'

National Cyber Security Centre (2018) 'Small Business Guide: Cyber Security'

This policy operates in conjunction with the following school policies:

Allegations of Abuse Against Staff Policy

Acceptable Use Agreement

Child-on-Child Abuse Policy

Anti-Bullying Policy

Staff Code of Conduct

Enabling Good Behaviour Policy

Disciplinary Policy and Procedures

Data Protection Policy

Photography and Images Policy

Prevent Duty Policy

Remote Education Policy

Safeguarding and Child Protection Policy

Social, Emotional and Mental Health (SEMH) Policy

2. Managing Online Safety

The importance of online safety is integrated across the school in the following ways:

Regular training for staff; online safety integrated into learning throughout the curriculum; assemblies and PSHE lessons conducted on the topic of remaining safe online

Handling online safety concerns Any disclosures made by pupils to staff members about online abuse, harassment or exploitation, whether they are the victim or disclosing on behalf of another child, will be handled in line with the Child Protection and Safeguarding Policy and/or the Child-on-Child Abuse Policy. Pupils, whether victims or perpetrators, will be supported accordingly.

Confidentiality will not be promised, and information may be shared lawfully if it is

in the public interest to share the information. The reasons for sharing the information will be explained and appropriate specialised support will be offered.

Concerns regarding a staff member's online behaviour will be reported to the headteacher, who will decide on the best course of action in line with the relevant policies. If the concern is about the headteacher, it will be reported to the Chair of Governors.

Concerns regarding a pupil's online behaviour will be reported to the DSL, who will investigate concerns in accordance with relevant policies depending on their nature, e.g. Enabling Good Behaviour Policy, Safeguarding Policy and Child Protection Policy, The Child-on-Child Abuse Policy.

Where there is a concern that illegal activity has taken place, the headteacher or DSL will contact the police. The school will avoid unnecessarily criminalising pupils, e.g. calling the police, where criminal behaviour is thought to be inadvertent and as a result of ignorance or normal developmental curiosity.

3. Cyberbullying Cyberbullying against pupils or staff is not tolerated. Incidents of cyberbullying will be dealt with quickly and effectively in line with the Anti-bullying Policy.

Cyberbullying can include, but is not limited to, the following:

Threatening, intimidating or upsetting text messages; threatening or embarrassing pictures and video clips sent via mobile phone cameras; silent or abusive phone calls or using the victim's phone to harass others, to make them think the victim is responsible; threatening or bullying emails, possibly sent using a pseudonym or someone else's name; unpleasant messages sent via instant messaging; unpleasant or defamatory information posted to blogs, personal websites and social networking sites, e.g. Facebook; abuse between young people in intimate relationships online i.e. teenage relationship abuse; discriminatory bullying online i.e. homophobia, racism, misogyny/misandry.

The school is aware that certain pupils can be more at risk of abuse and/or bullying online, such as LGBTQ+ pupils and pupils with SEND.

4. Child-on-child sexual abuse and harassment Staff understand that sexual abuse and harassment can occur both in and outside of school, off and online.

The following are examples of online harmful sexual behaviour of which staff will be expected to be aware:

Threatening, facilitating or encouraging sexual violence; upskirting, i.e. taking a picture underneath a person's clothing without consent and with the intention of viewing their genitals, breasts or buttocks; sexualised online bullying, e.g. sexual jokes or taunts; unwanted and unsolicited sexual comments and messages; consensual or non-consensual sharing of sexualised imagery; abuse between young people in intimate relationships online, i.e. teenage relationship abuse.

All staff promote a zero-tolerance approach to sexual harassment or abusive behaviour and will challenge such behaviour. Staff are aware that allowing such behaviour could lead to a school culture that normalises abuse and leads to pupils becoming less likely to report such conduct.

Staff are aware that creating, possessing, and distributing indecent imagery of other children, i.e. individuals under the age of 18, is a criminal offence, even where the imagery is created, possessed, and distributed with the permission of the child depicted, or by the child themselves.

The school will respond to all concerns regarding online child-on-child sexual abuse and harassment, regardless of whether the incident took place on the school premises or using school-owned equipment. Concerns regarding online child-on-child abuse will be reported to the DSL, who will investigate the matter in line with the Child-on-child Abuse Policy and the Safeguarding Policy Child Protection Policy.

5. Grooming and Exploitation Grooming is defined as the situation whereby an adult builds a relationship, trust and emotional connection with a child with the intention of manipulating, exploiting and/or abusing them.

Staff will be aware that grooming often takes place online and that pupils who are being groomed are commonly unlikely to report this behaviour for many reasons, e.g. the pupil may have been manipulated into feeling a strong bond with their groomer and may have feelings of loyalty, admiration, or love, as well as fear, distress and confusion.

The following are examples of online harmful sexual behaviour of which staff will be expected to be aware: Being secretive about how they are spending their time online; having an older boyfriend or girlfriend, usually one that does not attend the school and whom their close friends have not met; having money or new possessions, e.g. clothes and technological devices, that they cannot or will not explain.

Child sexual exploitation (CSE) and child criminal exploitation (CCE)

CSE involves sexual coercion and encouraging children to behave in sexually inappropriate ways through the internet. CCE is a form of exploitation in which children are forced or manipulated into committing crimes for the benefit of their abuser, e.g. drug transporting, shoplifting and serious violence. It is increasingly common for children to be groomed and manipulated into participating through the internet.

Where staff have any concerns about pupils with relation to CSE or CCE, they will bring these concerns to the DSL without delay, who will manage the situation in line with the Safeguarding Policy and Child Protection Policy.

Radicalisation

Radicalisation is the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups. Children who are targets for radicalisation are likely to be groomed by extremists online to the extent that they believe the extremist has their best interests at heart, making them more likely to adopt the same radical ideology.

Staff members will be aware of the factors which can place certain pupils at increased vulnerability to radicalisation, as outlined in the Prevent Duty Policy and are expected to exercise vigilance towards any pupils displaying indicators that they have been, or are being, radicalised.

Where staff have a concern about a pupil relating to radicalisation, they will report this to the DSL without delay, who will handle the situation in line with the Prevent Duty Policy.

6. Mental health

Staff are aware that online activity both in and outside of school can have a substantial impact on a pupil's mental state, both positively and negatively. The school's unique system of Consciousness-based Education places emphasis on the wellbeing of its pupils and staff: Why Maharishi School Is Unique

The school also has a fully trained Senior Mental Health Lead, a highly qualified Family Support Worker, trained Emotional Literacy Support Assistants and a trained Drawing and Talking Therapy practitioner.

Concerns about the mental health of a pupil will be dealt with in line with the Social, Emotional and Mental Health (SEMH) Policy.

7. Harmful online challenges For the purposes of this policy, **"harmful online challenges"** refers to challenges that are targeted at young people and generally involve users recording themselves participating in an online challenge, distributing the video through social media channels and daring others to do the same. Where staff suspect there may be a harmful online challenge circulating amongst pupils in the school, they will report this to the DSL immediately.

Where the DSL's assessment finds an online challenge to be putting pupils at risk of harm, they will ensure that the challenge is directly addressed to the relevant pupils, e.g. those within a particular age range that is directly affected or individual pupils at risk where appropriate.

The DSL and headteacher will only implement a school-wide approach to highlighting potential harms of an online challenge when the risk of needlessly increasing pupils' exposure to the risk is considered and mitigated as far as possible.

8. Online safety training for staff

The DSL ensures that all safeguarding training given to staff includes elements of online safety, including how the internet can facilitate abuse and exploitation. Staff are made aware that pupils are at risk of abuse, by their peers and by adults, online as well as in person, and that abuse can take place concurrently via online channels and in daily life.

9. Online safety and the curriculum

Regular practice of TM, and understanding of CbIDS, provides a sense of personal stability, providing a strong sense of self. This can act as a barrier between a user and online safety issues. In any unfortunate instances where such experiences have occurred, the practice of TM can help to restore imbalance caused by such stressful experiences.

Online safety is explicitly taught through Personal Social Health Education (PSHE), Relationships and Health Education (RHE)/Relationships, Sex and Health Education. Online safety teaching is always appropriate to pupils' ages and developmental stages.

The underpinning knowledge and behaviours pupils learn through the curriculum include the following: How to evaluate what they see online; how to recognise techniques used for persuasion; acceptable and unacceptable online behaviour; how to identify online risks; how and when to seek support

Class teachers will review external resources prior to using them to ensure they are appropriate for the cohort of pupils. External visitors, approved by the DSL and/or

the headteacher, may be invited into school to help with the delivery of certain aspects of the online safety curriculum.

If a staff member is concerned about anything pupils raise during online safety lessons and activities, they will make a report in line with the Safeguarding Policy and Child Protection Policy.

If a pupil makes a disclosure to a member of staff regarding online abuse following a lesson or activity, the staff member will make a report in line with the Safeguarding Policy and Child Protection Policy.

10. Use of technology in the classroom

Technology used during lessons will include chromebooks, including Google Classroom and Gmail. Cameras and mobile phones (secondary phase art/photography lessons) may be used.

Prior to using any websites, tools, apps or other online platforms in the classroom, or recommending that pupils use these platforms at home, the class teacher will review and evaluate the resource.

11. Use of smart technology

Primary phase pupils are not permitted to bring mobile phones or any other personal technology into school. Secondary phase pupils may bring mobile phones with them to school, however, these devices must be handed in at the start of the school day and can be collected at the end. Issues related to mobile phones are considered under the Mobile Phone Policy.

The school will address concerns related to the misuse of smart technology through assemblies and PSHE lessons, outlining the importance of using smart technology in an appropriate manner.

12. Working with parents

Internet issues will be handled sensitively to inform parents without undue alarm. Parents' attention will be drawn to issues of concern and useful links for parents via email and the school website.

13. Filtering and monitoring online activity

The school's ICT network has appropriate filters and monitoring systems in place. Staff will liaise with the headteacher (who will liaise with the IT technician) to ensure 'over blocking' does not lead to unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding. Reports of

inappropriate websites or materials will be made to the headteacher who will inform the IT technician immediately, ensuring any necessary changes are made.

The school will work in partnership with parents to ensure pupils stay safe online at school and at home. Parents will be made aware of the various ways in which their children may be at risk online.

14. Network security

Anti-virus software will be kept up-to-date and managed by the IT technician. Firewalls will be switched on at all times and reviewed at regular intervals. All staff have completed Cyber Awareness training, including the advice not to download unapproved software or open unfamiliar email attachments. Malware and virus attacks will be reported to the IT technician.

All members of staff and pupils have their own unique usernames and private passwords to access the school's systems. Staff members and pupils are responsible for keeping their passwords private.

Users will be required to lock access to devices and systems when they are not in use.

15. Emails

All staff members have a school email account to enable professional communication. This should not be used for personal emails and personal email accounts should not be used for work-related activities.

Pupils have a school email account and may contact staff via this medium to discuss school-related matters.

16. Social networking

Social networking is an increasingly popular way of communicating. When using social network sites, such as Facebook, Instagram or Twitter, members of staff need to be aware of the following good practice:

- Pupils should not be added as 'friends' on staff Facebook accounts and should not be able to access the contact of other social network accounts belonging to staff.
- Staff must not communicate with pupils using any digital technology where the content of the communication may be considered inappropriate or misinterpreted.
- Staff should not allow access by pupils or parents/carers to their social network accounts which may show their personal content that could be

considered unprofessional.

17. The school website

The headteacher is responsible for the overall content of the school website – they will ensure the content is appropriate, accurate, up-to-date and meets government requirements.

The website will be managed in line with the School Website Policy.

18. Remote learning

All remote learning will be delivered in line with the school's Remote Education Policy. This policy specifically sets out how online safety will be considered when delivering remote education.

19. Monitoring and review

The school recognises that the online world is constantly changing; therefore, the DSL, IT technician and headteacher will conduct termly light-touch reviews of this policy to evaluate its effectiveness.

The governing body, headteacher and DSL will review this policy in full on an annual basis and following any online safety incidents.

The next scheduled review date for this policy is March 2024.