**ONLINE SAFETY POLICY**

**POLICY AND PROCEDURES ON ONLINE SAFETY**

Policy Review Date: September 2022

| Version | Date | Updated By |
|---|---|---|
| 1.1 | January 2018 | M. Storey |
| 1.2 | September 2018 | G. Mann |
| 1.3 | September 2019 | G. Mann |
| 1.4 | September 2020 | G. Mann |
| 1.5 | September 2021 | S. Smith |

**The Wenlock School Online Safety Policy**

Online Safety encompasses internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences.

The Online Safety Policy has been revised to reflect the need to raise awareness of the safety issues associated with electronic communications as a whole.

The Wenlock School's Online Safety policy will operate in conjunction with other policies including those for Safeguarding, Management of Behaviour, Anti-Bullying, and the Curriculum.

**End to End Online Safety**

Online Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and pupils; encouraged by education and made explicit through published policies.
- Sound implementation of Online Safety policy in both administration and curriculum, including secure School network design and use.
- Safe and secure broadband from ZEN internet Limited including the effective management of Censornet and Fortigate filtering software. Specific blocks are updated daily. Additional websites as identified as inappropriate by staff can be blocked by contacting IT support.
- National Education Network standards and specifications.
- Specified authorities will be expected to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering.

**Online Safety policy**

Why Internet use is important:

- The Internet is an essential element in 21st century life for education, business and social interaction. The Wenlock School has a duty to provide pupils with quality Internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

**Teaching and Learning**

Internet use will enhance learning:

- School internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

**Pupils will be taught how to evaluate Internet content**

- The Wenlock School will ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.
- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

**Managing Internet Access**

Information system security:

- The Wenlock School ICT systems capacity and security are reviewed regularly.
- Filtering is via 'Fortigate' and 'Censornet' managed by ICT support.
- Virus protection is installed and updated regularly (Microsoft Security Essentials).
- The Fortigate software is primarily used to filter from a network level and will act as a backup should Censornet fail. Censornet filters on a local basis such as filtering sites for students. In addition, The Wenlock is using Netsupport software within the computing department providing options to filter and monitor individual devices / users.
- Security strategies are discussed with Outcomes First Group.

**E-mail**

- Pupils may only use approved e-mail accounts on The Wenlock School system.
- Pupils must immediately tell a member of staff if they receive an offensive e-mail.

- Pupils must not reveal personal details of themselves or others in e-mail communication or arrange to meet anyone without specific permission.
- E-mails sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on The Wenlock School headed paper.
- The forwarding of chain letters is not permitted.

**Published content and The Wenlock School web site**

- The contact details on the website should be The Wenlock School address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- The Headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

**Publishing pupil's images and work**

- Photographs that include pupils will be selected carefully; used only with parental, carers or pupil's written permission and will not enable individual pupils to be clearly identified.
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
- Work can only be published with the permission of the pupil and parents.

**Social networking and personal publishing**

- The Wenlock School will block/filter access to social networking sites (Facebook is blocked for all users on all school devices).
- Newsgroups will be blocked unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Pupils must not place personal photos on any social network space.
- Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and how to block unwanted communications. Pupils should be encouraged to invite known friends only and deny access to others.

**Managing filtering**

- The Wenlock School ensure systems to protect pupils are reviewed and improved through the use of Censornet and Fortigate Software and managed by IT support.
- If staff or pupils discover an unsuitable site, it must be reported to SLT or ICT support.
- Devices under the control of Lead tutors are checked regularly for web browsing history, and cleared, any concerns are reported to SLT or ICT support.
- The Senior Leadership Team will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

**Managing Videoconferencing and Web Cam**

As yet videoconferencing is not used at The Wenlock School; however, the following actions are identified as part of our safeguarding within our Online Safety policy:

- IP videoconferencing, School should check the broadband network to ensure quality of service and security.
- Pupils should ask permission from the supervising member of staff before making or answering a videoconference call.
- Videoconferencing will be appropriately supervised for the pupils' age.

**Managing emerging technologies**

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in The Wenlock School is allowed.
- Personal Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.

**Protecting personal data**

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

**Authorising Internet access**

- All staff must read the ICT policy for employees (located in the staff handbook) before using any Wenlock School ICT resource.
- All staff and pupils are granted access to The Wenlock School ICT systems.

- Pupils must accept Internet access individually by agreeing to comply with the Responsible Internet Use statement (*Appendix 1).*

**Assessing risks**

- The Wenlock School will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a Wenlock School computer. Neither The Wenlock School nor Outcomes First Group can accept liability for the material accessed, or any consequences of Internet access.
- The Wenlock School will audit ICT use to establish if the Online Safety policy is adequate and that the implementation of the Online Safety policy is appropriate.

**Handling Online Safety complaints**

- Complaints of Internet misuse will be dealt with by a member of the SLT.
- Any complaint about staff misuse must be referred to the Headteacher.
- Complaints of a child protection nature must be dealt with in accordance with The Wenlock School child protection procedures.
- The complaints procedure can be found on the school website.
- Advice will be sought from our local police as required to establish procedures for handling potentially illegal issues.

**Introducing the Online Safety policy to pupils**

- Pupils will be informed that network and Internet use will be monitored.
- Online Safety Assemblies are held regularly throughout the year.
- Pupils made aware of online extremism and radicalisation through assemblies and on-going work with West Midlands Police to highlight the dangers and signs of extremism and what pupils should do if they have concerns.
- Pupils are informed through these assemblies that Patrick Holness is the school Prevent Lead.
- All incidents of online safety will be reported via SLEUTH.

**Staff and the Online Safety policy**

- All staff will be asked to read The Wenlock School's Online Safety Policy.

- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct are essential.
- Staff that manage filtering systems or monitor ICT use will be supervised by the SLT and have clear procedures for reporting issues.
- Staff will receive PREVENT training delivered by West Midlands Police.

**Enlisting parent/carer support**

- Parents/carers attention will be drawn to The Wenlock School's Online Safety Policy by admission information, the prospectus and the school website.
- The Online Safety coordinator is the Lead of ICT and relays all concerns to the Designated Safeguarding Lead.
- Parents/carers are further informed of Online Safety awareness through the School Newsletter and through letters sent to parents/carers highlighting the Online Safety on social networks.
- Our Online Safety Policy has been written by The Wenlock School, building on government guidance. It has been agreed by the Senior Leadership Team.
- The Online Safety Policy and its implementation will be reviewed annually.

**Appendix 1**

Expectation & Guidelines for Responsible Internet Use

1. Treat your password like your toothbrush – keep it to yourself!

2. The messages you send will be polite and responsible. Do not use ICT to bully or harass others.

3. Only give your mobile number or personal website address to trusted friends.

4. Make sure you tell an adult of any unpleasant or inappropriate material or messages.

5. The school can check computer files and can monitor the internet sites visited.

6. Do not try to view, access, download or distribute unsuitable material.

7. Never install/download software in case we breach copyright laws or introduce viruses.

8. Never create or distribute images of anyone without their permission.

9. Refrain from using personal devices (mobile phone etc.) in school without permission.

10. Save the evidence: Learn how to keep records of offending text messages, pictures or online conversations.