Wise Owl Trust

Online Safety and Social Media Policy

Version 2

Approved by Wise Owl Trust: December 2017

Due for review: November 2019

Online Safety and Social Media Policy

Any parent/carer/adult with concerns regarding **any aspect of online safety** should report this to the Principal, Designated Safeguarding Lead or the Trust Computing Lead as a matter of urgency.

1. Introduction

"New technologies inspire children to be creative, communicate and learn. However, while the internet is a great resource, it is important that children and young people are protected from the risks they may encounter." DfE 2015

Across the Wise Owl Trust we understand the importance of the internet and how new technologies can enhance our children's learning experiences. We also recognise the safety implications of using such technologies and are therefore committed to ensuring that all our children, staff and families recognise how to use the internet and devices in a safe way. The Online Safety policy shows our commitment to keeping our children safe online and relates to other policies including those for Computing, Behaviour, Anti-Bullying, Safeguarding and Child Protection.

- The Trust Computing Lead will attend appropriate training and will provide support and training for all staff and volunteers across the three academies.
- The online safety policy will be reviewed annually and with reference to CPOMS (Child Protection Online Monitoring System) where a record will be kept of any inappropriate use of the internet.

2. Use of the Internet

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 administration systems. Internet use is part of the statutory curriculum and a necessary tool for learning. It is an essential element in 21st century life for education, business and social interaction. Access to the Internet is therefore an entitlement for pupils who show a responsible and mature approach to its use. Our Trust has a duty to provide pupils with quality Internet access. Pupils may use the Internet outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

2.1 How to ensure Internet use will enhance learning

- Each academy's internet access will be designed for pupil and teaching use and will include filtering policies appropriate to the age of our children, to ensure only safe websites can be accessed.
- Pupils will be taught what acceptable internet use is and given clear objectives on how to do so.
- Pupils will be educated in the effective use of the Internet as a research tool, including the skills of knowledge location, retrieval and evaluation.
- Parents can access further information regarding the Computing curriculum on the academy's websites.

2.2 Pupils will be taught how to evaluate internet content

- The academies will ensure pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations acknowledging sources of information used.
- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy. For example making pupils aware of the increase in 'Fake news' and websites on the internet and how to use their judgement to identify whether what they are reading is true or false.

3. Managing Internet Access

3.1 Information System Security

- Trust ICT systems capacity and security will be reviewed regularly.
- Virus protection will be updated regularly.
- No traffic shall enter or leave the Academy's Infrastructure without being explicitly permitted by the firewall. No traffic shall route directly between connected establishments unless it has been explicitly allowed to do so.
- Password security is of the utmost importance and must be maintained at all times. Adults and children will be reminded never to disclose their passwords. The abuse of passwords must be reported immediately to the Computing Trust Lead and recorded on CPOMS.

3.2 Managing filtering

- Developing good practice in internet use as a tool for teaching is essential. School internet access will be designed for pupil and teaching use and will include filtering policies appropriate to the age of the children.
- The Academies will work with Manchester City Council, DfE and internet provider service to ensure systems to protect pupils are reviewed and improved.
- Pupils cannot independently access YouTube.
- School iPads are set to the highest possible level of filtering so that children cannot access inappropriate content.
- No filtering system is perfect and pupils (and staff) will be taught what to do if they experience material they find distasteful, uncomfortable or threatening. This will be recorded on CPOMS and reported to the Online Safety Co-ordinator and the URL and content will be reported to the ICT service team.

3.3 Social Media platforms

- The Trust will control access to moderated social networking sites and educate pupils in their safe use.
- Our policy is to block/filter access to other social networking sites such as 'Facebook', 'Twitter', 'Instagram' etc. (Most have a minimum age of 13 specified).
- Pupils will be taught the importance of personal safety when using social networking sites, apps and chat rooms through assemblies and designated online safety lessons. They will be advised never to give out personal details of any kind which

may identify them or their location. They will be taught never to use a personal images of themselves.

- Pupils will be taught to never meet up with anyone they do not know. Older children will be instructed to always let an adult know if they are leaving the house and when they are likely to return.
- Pupils will be taught to consider the thoughts and feelings of others when publishing material to websites and elsewhere. Materials or comments which may be perceived to victimise or bully someone, or is otherwise offensive, is unacceptable and appropriate sanctions will be implemented. Any misuse will be recorded on CPOMS.
- Staff will not exchange personal social networking addresses or use social networking sites to communicate directly with pupils.

3.4 E-mail and other communications systems

- Pupils may only use approved, teacher supervised, e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail and this will be recorded on CPOMS.
- Pupils must not reveal personal details about themselves or others in e-mail communication. Arrangements to meet anyone will only be where it is part of a school project and pupils are working under the supervision of their teacher.
- Pupils will be taught about the dangers of computer viruses and how these can be transferred via email attachments.
- Personal e-mail or messaging between staff and pupils should not take place.

3.5 Published content and school website

- Editorial guidance will ensure that the Wise Owl Trust's ethos is reflected in each Academy's website and Twitter page, information is accurate, well presented and personal security is not compromised. Care will be taken to ensure that all information is considered from a security viewpoint including the use of photographic material.
- The contact details on the web site should be the academy address, e-mail and telephone number. Staff or pupils' personal information will not be published.

3.6 Publishing pupil's images and work

- Photographs that include pupils will be selected carefully and will not be labelled so individual pupils cannot be identified by the general viewing public.
- Written permission from parents or carers will be obtained before photographs of pupils are published on academy displays, printed publications by the academy or Wise Owl Trust, newspapers, academy or Wise Owl Trust websites, videos or social media.

3.7 Managing videoconferencing and/or direct online communication (SKYPE calls etc.)

- Video conferencing and/or direct online communications is only enabled through the use of Facetime or SKYPE.

- IP videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet.
- Only staff will be enabled to instigate a connection and thus check the suitability of the second party to the call.
- Pupils will be appropriately supervised whilst connected.

3.8 Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- When using YouTube staff will vigilantly ensure that;
    - It does not autoplay the next video.
    - They pre-watch the video ahead of time to ensure its content is age-appropriate.
    - They have the video prepared to play before the lesson so pupils cannot see side-panels or adverts on YouTube.
- Staff should not use mobile phones to take pictures or videos of children they should use their teacher iPad provided by the academy. These can be uploaded to the academy Twitter account or website.
- Mobile phones are not permitted for use anywhere in the academies, around the children except in exceptional circumstances. This applies to all members of staff and other visitors to the academies.
- Staff should take a mobile phone with them on a school trip/visit outside of school, for use in emergencies only.
- Children who bring mobile phones/tablets to the academies are required to hand them in to the school office staff every morning and devices are collected at home time.

3.9 Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
- Any personal data transported out of school on laptops, USB devices or other forms of storage will be encrypted and protected by password protection systems.

4 Policy decisions

4.1 Authorising Internet access

- All staff will sign an ‘Acceptable ICT use Agreement’ before using any school ICT resource.
- The academies will keep a record of any online safety issue or violations of the user policies on CPOMS. For instance a member of staff may discover unsuitable material that needs reporting or a pupil’s access may be withdrawn.
- At key stage one children’s experience of the internet will be through adult demonstration and access to websites under the supervision of an adult.

4.2 Assessing risks

- The academies will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on an academy computer. Our education programme for internet safety with pupils will give them clear strategies and processes for dealing with anything that causes them to feel uncomfortable.
- The Trust will audit ICT provision regularly to establish if the –safety policy is adequate and that its implementation is effective.

4.3 The Prevent Duty and Online safety

All schools have a duty to ensure that children are safe from terrorist and extremist material or radicalisation when accessing the internet in schools. We have an important role to play in equipping children to stay safe on line. Internet safety is integral to our Computing curriculum. Our staff are aware of the risks posed by online activity of extremists through training (e.g. Prevent) and have a duty to take action if they believe the well-being of any pupil or adult is being compromised.

5 Communicating the Policy

5.1 Introducing the Online Safety Policy to pupils

- Online safety rules will be posted in all networked rooms and discussed with the pupils at the start of each year.
- Pupils and staff will be informed that the network and internet use will be monitored and that misuse will be dealt with appropriately.
- Pupils and Parents will sign an Online Safety Agreement.
- Pupils will be taught appropriate and responsible behaviours for using the internet and communication tools within Computing, PSHCE and across the curriculum. Misuse will be recorded on CPOMS.
- Pupils will be instructed in responsible and safe use before being allowed access to the internet and will be regularly reminded of the rules and risks.

5.2 Staff and the Online Safety Policy

- All staff will be given the key points of the online safety policy and its importance explained. This will be part of the induction process for any new member of staff.
- Staff are made aware that internet traffic is monitored and traced to the individual user. Any potential misuse will be reported to the Trust and/or the police where appropriate. Discretion and professional conduct is essential.

5.3 Enlisting parents' support

- Parents will be asked to read through the online safety rules with their child. This will be signed by pupil and parent and returned to the relevant academy.
- Parental attention will be drawn to the Trust Online Safety Policy in newsletters, the academy brochure and on the school Web site.

6 Handling online safety concerns

- The staff, children and parents/carers will know how and where to report incidents (online safety coordinator, CPOMS and CEOP (Child Exploitation and Online Protection).
- Concerns related to safeguarding issues will be dealt with through the Trust's Safeguarding Policy and Procedures.
- Complaints of the internet misuse will be dealt with by a senior member of staff in accordance with the Trust Behaviour Policy.
- Any complaint about staff misuse must be referred to the relevant Principal and DSL.

7 Resources and Support for Parents and Children

Resources and support

In addition to any Local Safeguarding Children Board resources, the following resources can be used to support parents and children with youth produced sexual imagery.

Helplines and reporting

- Children can talk to a ChildLine counsellor 24 hours a day about anything that is worrying them by ringing 0800 11 11 or in an online chat at http://www.childline.org.uk/Talk/Chat/Pages/OnlineChat.aspx
- If parents or carers are concerned that their child is being contacted by adults as a result of having shared sexual imagery they should report to NCA-CEOP at www.ceop.police.uk/safety-centre
- ChildLine and the Internet Watch Foundation have partnered to help children get sexual or naked images removed from the internet. More information is available at http://www.childline.org.uk/explore/onlinesafety/pages/sexting.aspx
- If parents and carers are concerned about their child, they can contact the NSPCC Helpline by ringing 0808 800 5000, by emailing help@nspcc.org.uk, or by texting 88858. They can also ring the Online Safety Helpline by ringing 0808 800 5002.

Advice and information for parents

- The NSPCC has information and advice about sexting available on its website: https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/sexting
- NCA-CEOP has produced a film resource for parents and carers to help them prevent their children coming to harm through sharing sexual imagery: www.thinkuknow.co.uk/professionals/training/thinkuknow-introduction-course
- Childnet have information and advice about sexting available on its website: http://www.childnet.com/parents-and-carers
- Parent Info (www.parentinfo.org) provides information and advice to parents from expert organisations on topics ranging from sex and relationships, mental health and online safety. This includes content on sexting.
- The UK Safer Internet Centre have produced checklists for parents on using social networks safely www.saferinternet.org.uk/checklists

Resources parents could highlight to their children

- ChildLine have created Zip-It, an app that provides witty comebacks in order to help young person say no to requests for naked images - https://www.childline.org.uk/Play/GetInvolved/Pages/sexting-zipit-app.aspx
- There is information on the ChildLine website for young people about sexting: https://childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety/sexting/
- The Safer Internet Centre has produced resources called 'So You Got Naked Online' which help young people to handle incidents of sexting – https://www.cumbria.police.uk/Advice-Centre/Personal-Safety/Personal-Safety-Documents/So-you-go-naked-online-leaflet.pdf

Online Safety Agreement 2018 – 2019

Both pupils and their parents/carers are asked to sign to show that the online safety rules on the reverse of this agreement have been understood and agreed.

Consent for internet access and related technologies

I have read and understood the Trust's online safety rules and give permission for my child to access the internet and e-mail and message accounts as part of the school curriculum. I understand that the school:

- ✓ Will take all reasonable precautions to ensure that pupils cannot access inappropriate materials but I appreciate that this is a difficult task.
- ✓ Cannot be held responsible for the content of the materials accessed through the internet. I agree that the school is not liable for any damages arising from use of the internet facilities.
- ✓ May use monitoring software where this is available to ensure that inappropriate materials are being stored or used on school equipment.

I understand that if my child fails to follow the online safety rules that this may result in them not being permitted to use computers, the Internet and other new technologies in the academy.

Please print child's name _____

Parent/carers name (please print) _____

Signed by Parent/Carer _____ Date_____

Online safety Rules 2017 – 2018

Think then click

We use computers, the internet and lots of other new technologies to help us learn. To keep us safe when using them we must:

- ✓ Ask permission before using the internet
- ✓ Only use websites that an adult has chosen
- ✓ Immediately close any website we are unsure about
- ✓ Tell an adult if we see anything we are uncomfortable with
- ✓ Only e-mail and message people an adult has approved
- ✓ Only send emails and messages that are polite and friendly
- ✓ Do not open e-mails that are sent by anyone we do not know
- ✓ Never give out personal information of passwords
- ✓ Never arrange to meet anyone we do not know
- ✓ Do not use internet chat rooms or social networking sites

Pupil's agreement

- ✓ I have read and I understand the Online safety rules.
- ✓ I will use the computer, network, internet access and other new technologies in a responsible way at all times.
- ✓ I know that network and internet access can be monitored.
- ✓ If I fail to follow these rules, then I may not be allowed to use the computer, network, internet or other new technologies in school

Pupil name:_____ Class:_____

Signed by pupil_____ Date:_____