Manorbrook Primary School

Aiming for Excellence

Online Safety Policy

October 2023 Edition

The Internet and other technologies have the potential to offer many positive benefits to people of all ages. We want young people to be able to fully benefit from using the internet while doing so in a safe manner. Therefore, the purpose of this policy is to ensure that our school community is kept aware of the risks as well as the benefits of the internet and all associated online activity, and supported in managing these risks, in order to keep themselves and others safe

Our approach to online safety is based on addressing the following four key categories of risk, as outlined on pages 35 and 36 of KCSIE 2023:

- **Content:** being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.

- **Contact:** being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.

- **Conduct:** online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying, and

- **Commerce:** risks such as online gambling, inappropriate advertising, phishing and or financial scams. If we feel our pupils, students or staff are at risk, we will report it to the Anti-Phishing Working Group (link here)

Scope of the Policy

This policy applies to all members of the school community who have access to and are users of school ICT systems. It applies to systems in school and out of school where activities have been set by the school or are using school online systems. The Education and Inspections Act 2006 empowers Head teachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents such as cyber-bullying, which may take place out of school. The school will deal with such incidents in line with our behaviour and anti-bullying policies and will inform parents and carers of known incidents of inappropriate online behaviour that occur out of school. This policy should be read alongside the Acceptable Use Policies for staff and pupils.

Curriculum Provision

We believe it is crucial to educate children about how to behave responsibly online and how to keep themselves and others safe. Children and young people need the help and support of the school and parents to recognise and avoid online safety risks. As such, pupils receive online safety training every half-term throughout KS1 and KS2.

This programme of online safety learning can be found on the school's website, via this link:

https://primarysite-prod-sorted.s3.amazonaws.com/manorbrook-primary-school/UploadedDocument/4700fa49-80d1-4b1e-bb1c-eabae3ad0505/onlinonline safety-coverage-map-2022.pdf

As can be seen from the link above, our comprehensive programme is mapped out to ensure pupils receive relevant and helpful online safety training across a range of key themes:

Privacy and Security	Media Balance and Well-being	News and Media Literacy
Talking to Strangers	Online Information	Cyberbullying
Relationships and Communication		Digital Footprint and Identity

These themes are revisited as the pupils move through the school, consolidating their learning in order to keep them as safe as possible when online:

All the KS2 units and most of the KS1 units are taken from the following scheme:
https://www.commonsense.org/education/uk/digital-citizenship *

(*Common Sense Education is one of the recommended resource providers in the DfE's 'Education for a Connected World' Framework, 2020, which can be visited at the following link: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/896323/UKCIS_Education_for_a_Connected_World_.pdf)

All lessons within the 'Common Sense Digital Citizenship Scheme' contain clear, progressive learning objectives, and familiarise the children with the key vocabulary they will need to use the internet safely.

Online safety is also a focus in all areas of the curriculum where online activity is a feature, such as using the internet to support research in History and Geography, publishing work or studying authors in English, social skills in PSHE, data handling in maths and core skills in computing.

Key online safety messages may also be reinforced through some assemblies, and through activities for annual Safer Internet Day.

Students are given age-appropriate support to search safely and to evaluate the content that they access online, including considering the accuracy of information they find and use. Processes are in place for dealing with any unsuitable material that is found in internet searches. Pupils are also taught to acknowledge the sources of information they use and to respect copyright when using material accessed on the internet.

Staff are vigilant in monitoring the content of the websites the children visit and teach them to use specific search terms in order to reduce the likelihood of coming across unsuitable material.

Our behaviour policy may also be used to reinforce online behaviour.

Parents / Carers

Parents and carers have a critical role to play in supporting their children with managing online safety risks at home, reinforcing key messages about online safety and regulating their home experiences. However, some parents may wish to learn more about online safety issues or may feel unaware of risks and what to do about them.

The school supports parents to do this by giving parents clear Acceptable Use Policy guidance and providing them with useful web site links via the school website. The current list of recommended websites is taken from the September 2023 version of Keeping Children Safe in Education (page 159). It is copied here:

Online Safety - Parental Support

Childnet offers a toolkit to support parents and carers of children of any age to start discussions about their online life, and to find out where to get more help and support

Commonsensemedia provide independent reviews, age ratings, & other information about all types of media for children and their parents

Government advice about protecting children from specific online harms such as child sexual abuse, sexting, and cyberbullying

Internet Matters provide age-specific online safety checklists, guides on how to set parental controls, and practical tips to help children get the most out of their digital world

How Can I Help My Child? Marie Collins Foundation – Sexual Abuse Online

Let's Talk About It provides advice for parents and carers to keep children safe from online radicalisation

London Grid for Learning provides support for parents and carers to keep their children safe online, including tips to keep primary aged children safe online

Stopitnow resource from The Lucy Faithfull Foundation can be used by parents and carers who are concerned about someone's behaviour, including children who may be displaying concerning sexual behaviour (not just about online)

National Crime Agency/CEOP Thinkuknow provides support for parents and carers to keep their children safe online

Net-aware provides support for parents and carers from the NSPCC and O2, including a guide to social networks, apps and games

Parentzone provides help for parents and carers on how to keep their children safe online

Talking to your child about online sexual harassment: A guide for parents – This is the Children's Commissioner's parent guide on talking to your children about online sexual harassment

Education and Training - Staff and Governors

Training is provided to staff and governors to ensure they understand their responsibilities with regard to online safety. All new staff receive online safety training as part of their induction programme and refresh their online safety training regularly. Currently this training is provided by SSS Safeguarding.

The DSL (who is also the Online Safety Leader) receives regular updates through attendance at relevant training such as LA training sessions and by receiving regular online safety updates from South Gloucestershire Traded Services and Andrew Hall Safeguarding.

This Online Safety Policy and our Acceptable Use Policies may be discussed in staff meetings, as part of our standing item pertaining to safeguarding in all staff meetings.

The Computing Leader and the DSL provide advice/guidance and training as required to individuals as required and seek LA advice on issues where required, from the IT helpdesk.

Governors are able to access the same online safety training as staff through their SSS safeguarding training accounts.

Internet Provider, Monitoring and Filtering

The school uses Integra services to provide all necessary filtering and monitoring. Integra summarise their current support in the light of KCSIE 2023 in the following way:

"An updated version of Keeping Children Safe in Education (KCSiE) comes into force on the 1 September 2023. The updates include a new *emphasis on IT filtering and monitoring systems with a role for governing boards in making sure standards are met in this area.*
Integra, Schools IT have provided the following answers for schools who subscribe to their Broadband service.

1. Is your filtering provider:

a. A member of Internet Watch Foundation (IWF)?
Yes, the company we use that provides the filtering platform is a member of the IWF.

b. Signed up to Counter-Terrorism Internet Referral Unit list (CTIRU)?
Yes, the company provides a specific filtering category that contains this list.

c. Blocking access to illegal content including child sexual abuse material (CSAM)?
Yes, we use the categories provided by the filtering provider to ensure content is blocked.

In addition to the above, we use a separate reporting system that notifies us within 60 seconds if anyone on the network attempts to access any content on these lists.

2. Is the school's filtering operational and applied to all:

a. Users, including guest accounts?
Yes, our filtering monitors all devices using the wider network, regardless of who the device belongs to.

b. School owned devices?
Yes, our filtering monitors all devices using the wider network, regardless of who the device belongs to.

c. Devices using the school broadband connection?
Yes, our filtering monitors all devices using the wider network, regardless of who the device belongs to.

3. Does the filtering system:

a. Filter all internet feeds, including any backup connections?
Yes, our filtering monitors all devices using the wider network, regardless of who the device belongs to. All connections implemented or managed by Integra IT are subject to the filtering.

b. Be age and ability appropriate for the users, and be suitable for educational settings?
Yes, we utilise authentication to age-appropriate filtering. By default (with no authentication provided) the applied filtering levels are the most restrictive while being appropriate for the youngest users of the network.

c. Handle multilingual web content, images, common misspellings and abbreviations?
The filtering system is capable of handling all character sets (languages). It does not scan the content of images. Misspellings are included within the categories and can also be added manually.

d. Identify technologies and techniques that allow users to get around the filtering such as VPNs and proxy services and block them?
Yes, we are able to block based on category and application type, we have automated/dynamic application filters that automatically block all known and new/emerging bypass technologies (VPNs,
Proxy servers, etc…) for all users/devices on the network.

e. Provide alerts when any web content has been blocked?
Yes, all network & internet use is logged. All attempts to access blocked content or blocked applications or bypass attempts raise alerts. In addition to these we also block applications that are not deemed appropriate for use on the network, some of these applications (facebook, Instagram, twitter, etc…) are tied into many websites that are used everyday by schools, we do not generate alerts on these blocks as they are expected to occur.

4. Has the provider confirmed that filtering is being applied to mobile and app content?

Apps use many different methods to display their content. Some we are able to filter and others we cannot.

By default though, we block (in their entirety) mobile apps that are not specifically requested by schools.

5. Has a technical monitoring system been applied to devices using mobile or app content?

Schools can add additional monitoring to these devices if they wish.

6. Does the filtering system identify:

a. Device name or ID, IP address, and where possible, the individual? Yes

b. The time and date of attempted access? Yes

c. The search term or content being blocked? Yes

7. **Are there any additional levels of protection for users on top of the filtering service, for example, SafeSearch or a child-friendly search engine?**

   Yes, we enforce network wide SafeSearch (for all users) and restrict access to only search engines that fully support SafeSearch. This includes some mediated and/or child specific search engines, e.g. kiddle.co, kidrex.org, kidzsearch.com, safesearchkids.com, swiggle.org.uk, etc…

   Kiddle.co and kidzsearch.com are very good at providing safe image searches too!

8. **Does the monitoring system review user activity on school and college devices effectively? (For example, does it pick up incidents urgently, through alerts or observations, allowing prompt action to be taken; and is the response recorded)?**

   Yes, the monitoring system generates an alert within 60 seconds. Currently these alerts are sent to 3rd line IT staff for investigation. If the alert requires a response from school, a service ticket is generated and sent to the DSL for the school.

   We believe we have been able to tune most false positives out of the system, so our intention is to have these alerts raised directly to the DSL for investigation in the near future. It will never be possible to accurately remove all false positives from the system, but they have been sufficiently reduced to minimise unnecessary alert emails.

9. **Does the monitoring system ensure that incidents, whether of a malicious, technical, or safeguarding nature are picked up urgently?**

   The system generates the alerts as quickly as possible within 60 seconds. This ensures the relevant staff are aware that an incident needs to be investigated.

Requests from staff for sites to be removed from the filtered list must be approved by the head teacher. Any filtering requests for change and connected issues are reported immediately to the South Gloucestershire technical team on 3838.

Use of Digital Images and Video by Staff and Pupils

With the increased availability of mobile devices and tablets, taking and sharing images and video is much easier and, if not managed, this could increase the potential risk of misuse. The school informs and educates users about the risks associated with digital images.

- When using digital images, staff educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images, including on social networking sites.
- Pupils should not take, use, share, publish or distribute images / videos of others without their permission and staff reinforce this when appropriate.
- Staff are allowed to take digital / video images to support educational aims, but follow guidance in the acceptable use policy concerning the sharing, distribution and publication of those images.
- Photographs may not be taken on staff personal devices. They will be taken on school devices and forwarded to one of the school Facebook administrators, or a school website administrator, or stored on the school's drives for school use, e.g. for inclusion in a floor-book or a display.
- Facebook or website administrators will delete photos received on personal devices once they are uploaded.

- Parents sign permission forms to say that they will allow images to be taken of their child and used for educational purposes.
- Images are only taken and used of pupils where there is a signed permission form in place.
- Pupils' full names are not published on any online platform or school communication including the website, newsletter, Facebook. Prior to publishing, photographs are carefully selected and not used in association with pupils' full names or other information that could identify them, unless done so with express parental permission.
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use as this is not covered by the Data Protection Act. However, in order to protect other children and respect privacy these images should not be published or made publicly available on social networking sites. Parents / carers should also not comment on any activities involving other pupils in the digital / video images.

Data Protection

The school complies with the seven principles for storage of personal data outlined in Article 5 of the UK GDPR, which are as follows:
a) lawfulness, fairness and transparency, b) purpose limitation, c) data minimisation, d) accuracy, e) storage limitation, and f) integrity and confidentiality g) accountability
For more information: https://ico.org.uk/for-organisations/guide-to-data-protection

Staff ensure that they do the following: ensuring the safe keeping of personal data, minimising the risk of its loss or misuse; use personal data only on secure password protected computers / devices, ensuring that they are properly logged off at the end of a session using personal data; transferring data using encryption and secure password protected devices / memory sticks; deleting personal data from portable devices once they have finished with it.

Transfer of Data

Whenever possible secure online storage is used to ensure that documents do not need to be transferred to limit the risk. We ensure that data is stored in accordance with the requirements laid down by the Information Commissioner's Office and within the EU. This also applies to cloud storage used. The school's management of data is summarised in the school's data protection policy.

Passwords

All users of ICT systems log in with an individual user name to ensure that all only have access to the data they have a right to access. Passwords are managed by the technical support provider and any changes are logged. Users are told that passwords must never be shared for any IT system and that they are responsible for any actions taking using their log on.

Use of Personal Equipment in School

No pupils are allowed to use phones or mobile devices on the school premises.

Where staff have personal mobile equipment in school, they are never granted access to the school's wi-fi or school's drives, maintaining a barrier to protect all school and pupil information.

Staff must not use mobile phones for personal communication except when away from teaching or supervision responsibilities, e.g. at break times if not on duty. They must never communicate with pupils using their personal phones, and should always use school email for communication about school matters with parents and carers, and school phones for making calls to parents and carers, unless given permission by the head to do otherwise.

Staff personal mobile phones should not be used to store contact details of parents and pupils. Staff personal mobile phones are used to maintain contact when groups are away from the school site, or away from the main building (such as down in the woodland area). Mobile phones and personal devices are able to be used to support learning; this is managed by the class teacher and agreed with the head teacher. Staff must have regard to the Staff Acceptable Use policy in all matters relating to their online activity.

Reporting and Recording

There are clear reporting mechanisms in place for online safety incidents. All staff are reminded of these and fully aware of their responsibilities to follow up any reported issues.

- Online safety issues are reported to the DSL (who is the Online Safety Lead). If these include allegations of bullying then the anti-bullying policy is followed.
- Issues which may impact on the well-being and safety of a child are reported directly to the DSL, then Child Protection procedures are followed.
- Staff who are targeted by bullying online report these issues to the head teacher.
- Any member of staff seeing something online that is negative about the school reports this to the head teacher.
- Pupils are encouraged to report any incidents to an adult whether it relates to themselves or a friend. We encourage children to take responsibility for protecting each other, and teach all children to think of five trusted adults in school, to create a climate where sharing is as easy and non-threatening as possible
- If issues could be a result of problems with infrastructure or may affect it then the technical support provider is informed immediately (IT helpdesk ext: 3838).
- If access to an unsuitable site is reported then the Online Safety Lead will alert the technical support team by ringing 3838 to ensure that this is blocked.
- Serious incidents are escalated to local authority staff for advice and guidance.

- For incidents affecting school staff the Professionals Online Safety Helpline is contacted for advice if necessary on https://saferinternet.org.uk/professionals-online-safety-helpline or 0844 381 4772.

Any reported incidents are logged in the online safety log and followed up in accordance with the relevant policy depending on the issue. The response is also logged and serious issues are followed up after an interval of time to ensure that they are fully resolved.

Monitoring and Review

The policy will be reviewed every two years but may also be reviewed in response to new technologies being introduced or incidents that have taken place.

The school will monitor the impact of the policy using the following strategies:

- Logging of reported incidents and responses
- Discussions of online safety matters with pupils at class councils and school council
- Monitoring information about the teaching programme and coverage within the curriculum
- Regularly checking that pupils and staff are clear about how to report incidents and respond to them
- The content of the web site and Facebook page is regularly monitored by governors and senior leaders to ensure that it complies with this policy and the acceptable use policies.
- Any other web site that is linked to the school name will also be regularly monitored to ensure that the school is always presented accurately and professionally.

Review Frequency	1 years
Reviewed by	SLT
Latest version	October 2023
Approved by	Learning Committee
Next review due	October 2024

Appendix: Roles and Responsibilities

Role	Responsibility
Governors	Overall responsibility for ratifying the policy, ensuring that it is implemented and monitoring it. This action is delegated to the Learning Committee. Appoint an ICT governor to meet with the ICT leader, monitor and report on online safety practices
Head teacher and Senior Leaders:	Ensure that all staff receive suitable CPD to carry out their online safety roles and sufficient resource is allocated. Lead role in establishing / reviewing online safety policies / documents. Ensure that there is a system in place for monitoring online safety (via Integra IT). Follow correct procedure in the event of a serious online safety allegation being made against a member of staff Inform the local authority about any serious online safety issues Ensure that the school infrastructure / network is safe and secure and that policies and procedures approved within this policy are implemented. Provide regular training for staff (via SSS Safeguarding currently)
DSL (i.e. the Online Safety Lead):	Ensure all staff are aware of the procedures outlined in policies Attend updates and liaise with the LA online safety staff and technical staff as necessary Deal with and log online safety incidents including changes to filtering Meet with the Online Safety Governor to regularly to discuss incidents and actions arising

	Report regularly to the Senior Leadership Team
Curriculum Leaders	Ensure online safety is reflected in teaching programmes where relevant e.g. anti-bullying, English publishing and copyright and is reflected in relevant policies.
Teaching and Support Staff	Participate in any training and awareness-raising sessions Read, understand and sign the Staff Acceptable Use Agreement (AUP) Act in accordance with the AUP and online safety policy Report any suspected misuse or problem to the online safety Co-ordinator Monitor ICT activity in lessons, extra-curricular and extended school activities
Students / pupils	Participate in online safety activities Follow the acceptable use policy and report any suspected misuse Understand that the online safety Policy covers actions out of school that are related to their membership of the school
Parents and carers	Endorse (by signature) the Student / Pupil Acceptable Use Policy Ensure that their child / children follow acceptable use rules at home Discuss online safety issues with their child / children and monitor their home use of ICT systems (including mobile phones and games devices) and the internet Keep up to date with issues through school updates and attendance at events
Technical Support Provider	Ensure the school's ICT infrastructure is secure and is not open to misuse or malicious attack Ensure users may only access the school network through an enforced password protection policy, where passwords are regularly changed for those who access children's data Inform the head teacher of issues relating to the filtering applied by the Grid Keep up to date with online safety technical information and update others as relevant Ensure use of the network is regularly monitored in order that any misuse / attempted misuse can be reported to the Online safety Co-ordinator for investigation / action / sanction. Ensure monitoring software / systems are implemented and updated Ensure all security updates / patches are applied (including up to date anti-virus definitions and windows updates) and that reasonable attempts are made to prevent spyware and malware. Provision of temporary access of "guests" (e.g. supply teachers, trainee teachers, visitors) onto the school system is made through the use of supply log-ons.
Community Users	Sign and follow the AUP before being provided with access to school systems.