



Online Safety Policy

Policy Lead: Laura Theobald

Last reviewed on: October 2022

Approved by: Tammie Wisnia

Next review due: September 2023

Introduction

Online safety is an integral part of safeguarding and requires a whole school, cross-curricular approach and collaboration between key school leads. Accordingly, this policy is written in line with 'Keeping Children Safe in Education' 2022 (KCSIE), 'Teaching Online Safety in Schools' 2019, statutory RSHE guidance 2019 and other statutory documents. It complements existing and forthcoming subjects including Health, Relationships and Sex Education, Citizenship and Computing; it is designed to sit alongside the Kite Academy Trust Statutory Safeguarding Policy. Any issues and concerns with online safety must follow the school's safeguarding and child protection procedures. This policy applies to all members of the school community (including staff, children, governors, parents/carers, visitors and volunteers).

Aims

This Online Safety Policy explains the school's responsibility and approach to keeping children and adults safe, when using any devices linked to the internet. We aim to:

- Safeguard and protect all members of the Wyke Primary Academy community online.
- Identify approaches to educate and raise awareness of online safety throughout the community.
- Enable all staff to work safely and responsibly, including in the delivery of remote learning, 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.
- Clarify how the school implements planning and monitoring of the curriculum.
- Outline the roles and responsibilities of all members of the school community.
- Use of devices and equipment; data protection; social media; unsuitable and inappropriate activities and responding to inappropriate online incidents

Monitoring and Review

- Technology in this area evolves and changes rapidly. This school will review this policy at least annually. The policy will also be revised following any national or local policy requirements, any child protection concerns or any changes to the technical infrastructure.
- We will regularly monitor internet use and evaluate online safety mechanisms to ensure that this policy is consistently applied.
- To ensure they have oversight of online safety, the Headteacher will be informed of online safety concerns, as appropriate.
- The named governor for safeguarding will report on a regular basis to the governing body on online safety practice and incidents, including outcomes.
- Any issues identified via monitoring will be incorporated into our action planning.

Roles and responsibilities

The Head Teacher of Wyke Primary Academy will:

- Ensure all staff should be included in online safety training. Staff must also understand that misuse of the internet may lead to disciplinary action and possible dismissal.
- A designated member of staff for online safety is identified and receives appropriate on-going training, support and supervision and works closely with the Designated Safeguarding Lead.
- Ensures all temporary staff and volunteers are made aware of the school's Online Safety Policy and arrangements.
- Understand that online safety is an integral part of the safer recruitment and selection process of staff and volunteers.

The Governing Body will:

- Review the use and effectiveness of this policy. Governors receive regular information on online safety incidents and monitoring reports.

The Designated Member of Staff for online safety will:

- Along with the computing lead will monitor the online safety curriculum and the effectiveness of this.
- Regularly report any new information to the Senior Leadership Team and other colleagues.
- Provide training and advice for staff, children and parents/carers.
- Establish and review the school's Online Safety Policy and documents.
- Ensure all staff are aware of the procedures that will need to be followed in the event of an online safety incident taking place and how to report this.
- Liaise with school technical staff regarding and issues reported.
- Liaise with Headteacher about online safety incidents and logs of incidents to inform future planning of the curriculum.
- Attend relevant meetings and training.
- Update parents/carers via the newsletter and/or the website.

Kite Academy trust IT Support team are responsible for:

- Ensuring that the infrastructure is secure.
- Ensuring that the school meets the online safety technical requirements set out by the Local Authority.
- Ensuring all users have a secure log in with password protection, in which passwords are regularly changed.
- Keeping up to date with new information and making changes to the school's network in accordance to these changes, if appropriate.
- Monitoring the use and effectiveness of the software and systems in school and updating these regularly.

Teaching and Support Staff are responsible for:

- Being aware of their own personal responsibilities.
- Protecting the security and confidentiality of the school network, especially when working remotely at home.
- Teaching and following the online safety curriculum.
- Consistently referring to online safety rules during computing lessons and that these are displayed in the classroom
- Ensuring they lock their computers when they are not using them to prevent anyone else from accessing files.
- Ensuring they have read, understood and signed the Acceptable Use Agreement Code of Conduct for Staff Policy outlined by the Kite Academy Trust.
- Reporting any suspicions or concerns to the Headteacher.
- Ensuring all digital communications with parents/carers are on a professional level and through the school's online learning platforms; SeeSaw, Tapestry and the relevant year group email addresses.
- Ensuring online safety is embedded across other curriculum areas as they arise.
- Ensuring children have a good understanding of research skills and use of search engines.
- Ensuring children are aware of copyright and plagiarism.
- Ensuring visitors and volunteers are aware of current policies, particularly on school trips and with the use of technological devices, mobile phones and cameras.
- Ensuring internet use in lessons is pre-planned and websites have been checked before children view them.
- Ensuring children know what they can and cannot access at all times.
- Ensuring children are not left alone with iPads or any other devices connected to the Internet.

All staff are responsible for:

Whenever the children use technology in its various forms, all staff within the school will protect and ensure that every child in their care is safe from dangers such as:

- The use of internet for grooming children and young people with the ultimate aim of exploiting them sexually
- The use of technology as a new weapon for bullies, who may torment their victims via websites, text messages or exposure to inappropriate content when online, which can sometimes lead to involvement in crime and anti-social behaviour.

Children are responsible for:

- Using the school's digital systems appropriately and in accordance to the online safety rules and regulations.
- Having a good understanding of how they can report incidents or concerns.
- Having good understanding of what is appropriate and what is not.
- Understanding the importance of good online safety practice when using digital devices inside and outside of school.

Parents/Carers:

Parents/carers play a crucial role in ensuring children are fully aware of how to be safe online and monitoring this. The school will provide updates and advice for parents/carers through parents' evening, newsletters, letters, and the school website. Parents/carers are encouraged to promote good online safety practice and follow the guidelines set by the school.

Visitors/ Supply Teachers:

- Are provided with a secure log in when they come into school.
- Staff will monitor visitors conduct with regards to online safety and it will be their responsibility to raise concerns

Curriculum

At Wyke, we follow Project Evolve, an Online Safety Curriculum program. This covers all key areas of online safety and has been devised to ensure that there is a progression of skills and that children receive a broad and balanced curriculum.

These key areas are:

- Self-image and identity
- Online relationships
- Online reputation
- Online bullying
- Managing online information
- Health, well-being and lifestyle
- Privacy and security
- Copyright and ownership

Resources are provided through Project Evolve for teachers to use. Online safety is embedded through explicit teaching, as an integral part of each computing lesson and other areas of the well-being when appropriate. The online safety curriculum is also delivered through the Personal, Social and Health Education (Jigsaw) and is a subject which is frequently revisited. Children are made aware of the impact of bullying and this is intertwined with cyber bullying.

Children are taught in lessons to be critically aware of search engines and the reliability of sources as well as other materials and content they access online. It may be difficult for children to determine the origin, intent and accuracy of information; therefore, it is vital that they are educated on this. The children are made aware that the internet also contains 'fake news' which is unreliable and inaccurate. Children are guided to research sites which are age appropriate and suitable for given tasks.

In addition to this, the children are also educated on plagiarism and copyright and the rules and regulations when accessing information on the internet. Where children are allowed to use the internet for research purposes, staff should be vigilant in monitoring the content they are visiting.

Education for Parents/Carers:

It is important that parents/carers feel they can approach the school with questions in regards to keeping their child/children safe online. At Wyke Primary Academy, we provide information to parents and carers through a range of platforms:

- Letters
- Newsletters
- School website
- Parents' Evenings
- Safer Internet Day
- Reference to particular websites of use to parents

Parents/carers are directed towards the parent code of conduct on the school website when their child starts at school. This has details of the use of inappropriate social media use.

<https://www.thekiteacademytrust.org/assets/Documents/Policies/KAT-Code-of-Conduct-for-Families.pdf>

Education for Staff/Volunteers:

It is vital that staff are kept up to date with important key messages in relation to online safety. Staff are regularly updated with new information by either the Leadership Team or the Online Safety/Computing Lead. This may include training and links to resources. All staff are required to have read and acknowledged the Online Safety Policy. Any updates and changes to the Online Safety Policy will be discussed with staff, and updates are sent regularly, for example via email.

The Kite Academy Trust IT Technical and Network team are also provided with training as and when required, in order to ensure the school system is running correctly and any updates are actioned.

Managing Internet Access

The Kite Academy Trust IT Technical and Network team ensures that certain web addresses are filtered and any new websites which may be reported are also filtered, if they are deemed unsuitable for school use. The filters set in place ensure that the children and staff are safe from potentially damaging material. At Wyke Primary Academy we use SurfProtect to monitor online use. This is monitored weekly by the DSL. Any repeated searches (5 or more times in one hour) that breach the filtering criteria will result in an immediate email to alert the DSL. They will access the monitoring system to establish where this has happened and this will then be dealt with accordingly.

If internet research is set as a home learning task, teachers will provide specific links in which children could use. These would have been checked by teachers to ensure the content is appropriate and suitable for the age group in question.

Staff are fully aware that the school's email and internet system can be monitored and explored further if required.

If staff or children do discover an inappropriate website, it must be reported to the Kite Academy Trust IT Technicians immediately and the screen turned off to prevent anyone else from seeing the information.

Security and Data Protection:

Personal data will be used and stored in accordance with General Data Protection Regulations which states that personal data must be stored:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than necessary
- Processed in accordance with the data subject's rights.
- Secure
- Only transferred to others with adequate protection.

School staff are required to read and confirm they will comply with the Kite Academy Trust Data Protection (GDPR) & Freedom of Information Policy. They are responsible for:

- Collecting, storing and processing any personal data in accordance with that policy
- Informing the school of any changes to their personal data, such as a change of address

They will be required to contact the Data Protection Officer in the following circumstances:

- With any questions about the operation of that policy, data protection law, retaining personal data or keeping personal data secure
- If they have any concerns about that policy is not being followed
- If they are unsure whether or not they have a lawful basis to use personal data in a particular way
- If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
- If there has been a data breach
- Whenever they are engaging in a new activity that may affect the privacy rights of individuals or if they need help with any contracts or sharing personal data with third parties

In order to comply with regulations, at Wyke Primary Academy we will ensure that:

- Staff do not share personal/school data with anyone else (even when they are no longer an employee) unless required for specific reasons as stated in the Kite Academy Trust Data Protection (GDPR) & Freedom of Information Policy.
- All staff passwords will be individual passwords and will not be shared with other members of the school community or written down
- Staff passwords are changed regularly
- When unattended, all computers and laptops are logged off properly or locked using 'windows & L'.
- All computers and laptops are shut down at the end of the day and stored appropriately if necessary.

- Emails from external addresses are made known in the subject to staff when they open their email box. Emails from suspicious sources are not opened. These should be reported to the Kite Academy Trust IT Technical and Network team who will de-bug these emails.
- Photographs of children are only taken and saved on the network where permission to do so has been granted by parents.
- The security of the school information systems and users are regularly reviewed.
- Virus protection is regularly updated.
- Unapproved software is not allowed.
- Mobile phones are not used to take photographs of children, only authorised school cameras and in line with the school policy for using photographic images.
- Websites are investigated before directing the children to use them.

Use of Digital and Video Images

- Written permission from parents/carers will be obtained before photographs of children are taken and published.
- Staff and volunteers are not permitted to use their devices to take or record images of children, any photography or videos must be taken using an approved school device.
- Care should be taken when taking photographs and videos to ensure that children are appropriately dressed and not participating in activities which might bring the school into disrepute.
- Photographs published on the school's website or elsewhere will be chosen carefully and comply with good practice.
- Children's full names will not be published with the photograph.

Social Media

At Wyke Primary Academy we are aware of the increase in different types of social media and children's use of it, possibly underage. We educate children through online safety lessons about appropriate use of these sites and sharing personal information. We have the following measures in place:

- Inappropriate social networking sites are blocked in school.
- Staff and children are not permitted to use sites on school computers or devices.
- Training is provided for the Online Safety/Computing Lead and updates filtered through to staff.
- Clear reporting and filtering of sites.
- Where filtering is not possible (on iPads), children are not left alone with the device at any times.

Staff Use

- Staff should not refer to children, parents/carers or the school and other staff members on their personal accounts.
- Staff should not engage in online discussions about personal matters relating to school life, children and their families.

- Staff should keep personal opinions to themselves, with regard to the school community or education generally, in case these views are taken as representing the school.
- Staff should ensure that settings on social media are appropriate and regularly checked to minimise risk.

If there are any concerns in regard to children's use of social networking (in or out of school), they will be reported to the Designated Safeguarding Lead and concerns will be shared with parents/carers.

As a school, we have social media pages, which enable us to share information and events within school. These social media pages only have images of children whose parents have given their consent.

Use of Mobile Devices

The use of mobile phones by children is not permitted in school. If a child has brought in a mobile phone they must be switched off during school hours, collected in by the Class Teacher and taken to the School Office where they will be secured in a locked draw.

Staff are permitted to have their mobile phones in school and use them during lunch and break time when they are not in the company of children. During teaching times these must be out of sight. In case of emergency, staff may be contacted via the School Office. Volunteers and visitors are also briefed on the school's rules about mobile phones and must follow these rules as well. Staff are not permitted to use their own personal devices for contacting children or their families within or outside of the school setting. The exception for this is when staff are working remotely, on residential trips or in other extreme circumstances. In these cases, when using personal devices, the Caller ID is withheld.

Reporting and Responding to Incidents of Misuse

It is vital that the school works in partnership with families in order to educate the children on online safety. Even though we have protection systems in place, incidents can occur. Due to the rise of internet and technology use in society, it is always a concern that children are naïve to potential dangers and risks. Concerns or incidents are reported through the right channels to ensure that we are addressing these issues within our curriculum.

Material can appear briefly on computers even if there are filtering services in place. The school cannot be held liable for this however any complaints in relation to this do need to be made to the Head teacher.

Online safety is part of safeguarding and therefore should be reported directly to the Designated Safeguarding Lead. This information will then be passed onto the relevant members or staff and parents/carers contacted if needed. Incidents are then logged.

Authorising Internet Access

- All staff must read and sign to acknowledge that they have read and agree to uphold the intentions of this policy.

- All parents and children will be asked to sign and return a consent form agreeing to 'Responsible Use.'
*See appendix 2.
- The Kite Academy Trust IT Technical and Network will maintain a current record of all staff and children who are granted access to school computing systems.
- At both key stages, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials. There will be occasional 'free time' to research topics which will be supervised by an adult.

- Any person working in school regularly i.e. students or parent helpers not directly employed by the school will be asked to read and sign the guidance and policy on use of technology before being allowed to access the Internet from the school site.
- Children will have the online rules shared with them regularly. *See appendix 1.
- This policy will be shared with children and parents with regular reminders and published on the school website.
- Any complaint about staff misuse must be referred to the Head Teacher.
- Any complaint about misuse by the Head Teacher should be referred to the Chair of Governors.

Appendix 1

Wyke Primary Academy Online Safety Rules

BE SMART ONLINE!

Secret- Keep personal details, such as home or school address, telephone numbers and age private.

Messages- Only contact people you know online. Keep messages, polite, sensible and kind.

Acept- Ask before you use the internet and do not accept or open anything you are unsure of.

Reliable- Do not trust everything you read online and check your facts.

Tell- An adult if you see or hear anything on the computer that makes you feel uncomfortable or doesn't seem right.

Appendix 2

Policies/ useful links

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1021914/KCSIE_2021_September_guidance.pdf

<https://www.gov.uk/government/publications/relationships-education-relationships-and-sex-education-rse-and-health-education>

<https://www.thekiteacademytrust.org/assets/Documents/Policies/KAT-Data-Protection-GDPR-Freedom-of-Information-Policy.pdf>

<https://www.thekiteacademytrust.org/assets/Documents/Policies/KAT-Safeguarding-Child-Protection-Policy.pdf>

<https://www.thekiteacademytrust.org/assets/Documents/Policies/KAT-Relationships-Sex-Education-Policy.pdf>

<https://www.thekiteacademytrust.org/assets/Documents/Policies/KAT-Code-of-Conduct-for-Families.pdf>

<https://www.thekiteacademytrust.org/assets/Documents/Policies/KAT-Code-of-Conduct-for-Governors-Staff.pdf>