Woodend Farm school

Kindness comes in many forms

Online Safety

Version: October 2025 V1.5

Original Issued: August 2022

Original Author: Gemma Quantrill & Nicola Overland

RECORD OF POLICY AMENDMENT / HISTORY

Version / Issue	Updated by	Date	Reviewed/ Approved By Governors	Reason for Change
V1.0 – Initial draft	Gemma Quantrill	17/08/22	26/01/2023	New Policy
V 1.1	Nicola Overland	31/10/2023	08/11/2023	Annual review
V 1.2	Nicola Overland	20/3/2024		Updates from Online Safety Act and KCSIE (2023)
V1.3	Nicola Overland	24/10/2024		Annual updates
V1.4	Gemma Quantrill	29/09/25		Annual updates
V1.5	Gemma Quantrill	10/10/25		Amendment to job titles

1. The purpose of this policy

This policy reflects the latest guidance from *Keeping Children Safe in Education (2025)* and the *Online Safety Act*, ensuring that pupils across both primary and secondary phases are supported to navigate digital spaces safely and responsibly.

Woodend Farm School works with children and families and has a responsibility to ensure that children and young people can use the internet and related communications technologies appropriately and safely. This is addressed as part of the wider duty of care to which all who work in schools are bound. Research has shown that the use of these exciting and innovative tools, used in school and at home, demonstrates a rise in educational standards and to promote pupil/student independence and achievement.

However, the use of these technologies can put young people at risk within and outside the school environment. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content.
- Un-authorised access to / loss of / sharing of personal information.
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge.
- Inappropriate communication / contact with others, including strangers.
- Cyber-bullying.
- Access to unsuitable video / internet games.
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the offline world and it is essential that this policy is used in conjunction with other relevant school policies such as behaviour, anti-bullying and safeguarding.

It is impossible to eliminate those risks completely. It is therefore essential to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to manage these risks independently as they develop into young adults.

This policy supports this by identifying the risks and the steps we are taking to avoid them. The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk as stated within Keeping Children Safe in Education:

- 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: personal 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 you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group. Details can be found at www.apwg.org.

(DfE Keeping Children Safe in Education 2024)

2. Scope of the Policy

This policy applies to all members of the school community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school.

The Education and Inspections Act 2006 empowers headteachers, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other on-line e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

The 2011 Education Act increased these powers with regard to the search for and of electronic devices and the deletion of data. In the case of both these acts, action can only be taken in relation to our published Behaviour Policy. The school will deal with such incidents within this policy and associated behaviour and antibullying policies and will, where known, inform parents / carers of incidents of inappropriate online behaviour that takes place out of school.

3. Roles and Responsibilities

Board of Governors

Governors are responsible for the approval of the Online Safety Policy and for reviewing its effectiveness.

Executive Headteacher

- The Executive Headteacher is responsible for ensuring the safety (including online safety) of members of the school community and the day-to-day responsibility for online safety as part of their role as DSL.
- The Executive Headteacher is responsible for the implementation and effectiveness of this policy. She is also responsible for reporting to the board of Governors on the effectiveness of the policy and, if necessary, make any necessary recommendations regarding further improvement.
- The Executive Headteacher / Senior Leaders are responsible for ensuring that staff receive suitable CPD to enable them to carry out their roles.
- The Executive Headteacher / Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Executive Headteacher and another member of the Senior Leadership should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (See Managing Allegations against a member of staff policy/guidance)
- The Executive Headteacher is responsible for ensuring that parents and carers, when given access to data and information relating to their child / children, via any cloud-based website, Learning Platform or Gateway, have adequate information and guidance relating to the safe and appropriate use of this online facility.
- The Executive Headteacher is responsible for ensuring age-appropriate implementation of online safety education and monitoring within their respective phases.
- Therapeutic staff, including Thrive practitioners and behaviour mentors, support pupils in understanding online risks through relational and restorative approaches.

Designated Safeguarding Lead

Designated Safeguarding Lead:

- Take day to day responsibility for online safety issues and have a leading role in establishing and reviewing the school online safety policies / documents
- Ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place
- The DSL is responsible for understanding the filtering and monitoring systems and processes in place.
- Report to the School Leadership Team serious breaches of the Online Safety and related policies.
- Provide ongoing training and advice for staff.
- Liaise with the Local Authority
- Receive reports of online safety incidents and create a log of incidents to inform future safety developments
- Are trained in and share with staff an awareness and understanding of online safety issues and the potential for serious child protection issues that can arise from:
    - Sharing of personal data
    - Access to illegal / inappropriate materials
    - Inappropriate on-line contact with adults / strangers
    - Potential or actual incidents of grooming
    - Cyber-bullying
    - Sexting
    - Revenge pornography
    - Radicalisation (extreme views)
    - CSE

- Ensure that staff training includes filtering and monitoring.

Teaching and Support Staff

Teaching and Support Staff are responsible for ensuring that:

- They have an up-to-date awareness of online safety matters and of the current school online safety policy and practices
- They have read, understood and signed the Online Safety Policy and school Staff Acceptable Use of Technology Policy / Agreement (AUP)
- They report any suspected misuse or problem to the Designated Safeguarding Lead for investigation / action / sanction
- Digital communications with pupils and parents / carers (email / voice) should be on a professional level
- Students / pupils understand and follow, as appropriate for age and ability, the school Online Safety and acceptable use policy
- Students/ pupils understand and follow Online Safety rules and they know that if these are not adhered to, sanctions will be implemented in line with our promoting positive behaviour and anti-bullying policies.
- In lessons where internet use is planned students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Pupils

- Are responsible for using the school ICT systems in accordance with the Student / Pupil Acceptable Use Policy, which they will be expected to agree to before being given access to school systems, where appropriate for age and ability.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so, where appropriate for age and ability.
- Will be expected to follow school rules relating to this policy for example, safe use of cameras, cyber-bullying etc.
- Should understand that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school, where appropriate to their age and ability.

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through parents' evenings, letters, website / local online safety campaigns / literature. Parents and carers will be responsible for:

- Endorsing (by signature) the Pupil Acceptable Use Agreement *(see appendix A)*
- Accessing the school website/on-line pupil records/school social media in accordance with the relevant school Acceptable Use Policy.

Parents/carers should understand that school has a duty of care to all pupils. The misuse of non-school provided systems, out of hours, will be investigated by the school in line with our behaviour, anti-bullying and child protection and safeguarding policies.

4. Development and Monitoring

Role	Named Person	Contact
Designated Safeguarding Lead	Gemma Quantrill	gquantrill@woodendfarm.school
Deputy Designated Safeguarding Lead	Anna Kinsville	akinsville@woodendfarm.school
Network Manager	Immersive IT	support@immersive-it.co.uk

This e-safety policy has been developed by the Designated Safeguarding Lead in conjunction with the School Leadership team and the Network Manager. As part of this policy, records will be maintained of online safety related incidents involving staff and pupils and any incidents recorded will be treated in accordance with our safeguarding procedures. This policy will be reviewed at least annually.

The school will monitor the impact of the policy using:

- Feedback from staff, pupils, parents / carers, governors
- Logs of reported incidents
- Internet activity monitoring logs

Monitoring will include feedback from primary and secondary pupils, ensuring that online safety education is relevant, accessible, and responsive to their lived experiences.

5. Education and Training

Education – Pupils

Online Safety education will be provided in the following ways, as appropriate to pupils' age and ability:

- A planned online safety programme will be provided as part of PHSE and will be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school
- Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial activities. Outside agencies may also deliver some of this programme
- Pupils should be encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet, as appropriate to their age and ability
- Pupils are taught the importance of keeping information such as their password safe and secure.
- Rules for the use of ICT systems / internet will be made available for pupils to read, in writing and in symbol format
- Staff should act as good role models in their use of ICT, the internet and mobile devices
- Where pupils are allowed to freely search the internet, e.g. using search engines, staff will be vigilant in monitoring the content of the websites the young people visit in line with Woodend Farm School policies (Smoothwall web filtering is also used to block inappropriate internet search terms)
- It is accepted that from time to time, for good educational reasons, pupils may need to research topics (e.g. racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Network Manager (and other relevant person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, will be auditable, with clear reasons for the need and will be retained for review to ensure it complies with the policy.
- Online safety education will be adapted for primary and secondary pupils, using symbol-supported resources, social stories, and scenario-based learning where appropriate.

Education – Parents and Carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's online experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it.

Woodend Farm School will therefore seek to provide information and awareness to parents and carers through:

- Letters, website and social media.
- Parents evenings.
- Reference to external websites.
- High profile events such as Internet Safety Days.
- Family learning opportunities.

Workshops and resources will be tailored to the needs of families with children in both primary and secondary phases, including those with additional needs.

Education and Training – Staff

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal online safety training will be made available to staff. An audit of the online safety training needs of all staff will be carried out regularly.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand and agree to adhere to the school Online Safety and Acceptable Use policies
- The Online Safety Coordinator (or other nominated person) will provide advice/guidance/training to individuals as required.

Staff will receive training on how to deliver online safety education in a trauma-responsive and developmentally appropriate way.

6. Technical – Infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

- Servers, network hardware and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to school ICT systems.
- Staff will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- Staff will use secure passwords to access the network, ensuring that these are not easily guessable.
- Staff using OneDrive to access the school network from home will keep their passwords secure and not allow members of their household to access the system. They will logout of the network at the end of each session.
- The school maintains and supports the Smoothwall filtering service. Any incidents or activities regarding filtering will be handled in accordance with school safeguarding policies.
- Securus, a highly effective monitoring system which identifies cyberbullying and other safeguarding concerns is used in school. The report logs are checked weekly by the Network Manager and any issues that are highlighted in these checks are written in the Online Safety.
- Log and reported to Designated Safeguarding Lead.
- Appropriate security measures are in place to protect the servers, routers, wireless systems, workstations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data.
- The school infrastructure and individual workstations are protected by up-to-date antivirus software.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured in accordance with the school Personal Data Policy.

7. Use of Digital Photographs and Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet / social media. Those images may remain available on the

- internet forever and may cause harm or embarrassment to individuals in the short or longer term. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- Staff are allowed to take digital/video images to support educational aims, but must follow school policies concerning the storing, sharing, distribution and publication of those images. Those images should only be taken on school equipment. The personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
  Written permission from parents or carers will be obtained before photographs of students/pupils
  together with their name displayed alongside are published in leaflets, posters, documents, training materials or used by the press.
- Written permission from parents or carers will be obtained when a pupil starts school before photographs of students/pupils are published on the school website or social media. This permission can be withdrawn at any time. Students' / Pupils' full names will not be used anywhere on a website or social media, particularly in association with photographs.
- Photographs published on the website, or elsewhere that include students/ pupils will be selected carefully and will comply with good practice guidance on the use of such images.

Consent for image use is reviewed annually and can be withdrawn at any time. Staff are reminded to avoid capturing images of pupils in distress or during therapeutic interventions.

8. Data Protection

Personal data will be recorded, processed, transferred, and made available according to the Data Protection Act 2018. More detailed guidance on the collection, handling and storage of personal data can be found in the school's Data Protection Policy.

In summary, personal data will be:

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

Staff must be aware that a breach of the Data Protection Act may result in the school or an individual fine. All staff will complete annual data protection training, including secure handling of digital records and cloud-based systems such as CPOMS and Evidence for Learning. Staff must also ensure that they:

- Take care at all times to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Access personal data on secure password protected computers and other devices or via any online Learning Platform, OneDrive, Evidence for Learning or CPOMS ensuring that they are properly "logged-off" at the end of any session in which they are using personal data
- Transfer data using encryption and secure password protected devices
- Do not share passwords internally or externally
- When personal data is stored on any portable computer system, USB stick or any other removable media.

- Data must be encrypted, and password protected
- The device must be password protected (many memory sticks / cards and other mobile devices cannot be password protected.)
- The device must offer approved virus and malware checking software
- The data must be securely deleted from the device, in line with school policy once it is no longer required.

9. Communications

When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure. Pupils should therefore not use other email systems when in school, or on school systems.
- Users need to be aware that email communications may be monitored.
- Users must immediately report to the Online Safety Coordinator – in accordance with this policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff, pupils or parents / carers must be professional in tone and content and be via official used systems.
- Individual email addresses will be provided to some pupils if deemed appropriate for their level of ability by their class teacher.
- Pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be placed on the school website on public facing calendars and only official school emails should be identified within it.
- The school allows staff to bring in their own personal devices, including mobile phones, for their own use. Under no circumstances should a member of staff use their personal devices including mobile phones, to contact a pupil, parent/carer
- The school is not responsible for the loss, damage or theft of any personal mobile device
- The sending of inappropriate text messages between any member of the school community is not allowed.
- Users bringing personal devices into the school must ensure there is no inappropriate or illegal content on the device. Other 'social networking' facilities may be 'unfiltered' for curriculum purposes. Staff are aware of the procedure they need to follow when requesting access to externally based social networking sites.
- Staff are prohibited from using AI chatbots or messaging apps to communicate with pupils. Any use of AI tools for educational purposes must be approved by the Executive Headteacher and comply with data protection policies

10. Responding to incidents of misuse

There may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If any apparent or actual misuse by pupils, staff or any other user appears to involve illegal activity i.e.

- Child sexual abuse images
- Adult material which potentially breaches the Obscene Publications Act
- Criminally racist material
- Other criminal conduct, activity or materials

All incidents will be logged on CPOMS and reviewed by the DSL. Where necessary, referrals will be made to the Essex Family Operations Hub or the Police Cyber Crime Unit.

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner.

End of Document