A place for fun, creativity, friendship, ambition and discovery

Online Safety and Acceptable Use Policy

1. Purpose and scope

Digital technology, the internet and online communication provide valuable opportunities for learning, creativity and connection. They also bring risks. Children may encounter unsuitable content, harmful communication, misinformation, scams, inappropriate contact, cyberbullying and attempts to obtain personal information.

Langham Village School is committed to helping pupils develop the knowledge and skills to use technology safely, responsibly and confidently. This policy sets out expectations for pupils, staff, governors, volunteers, parents and other adults using the school's systems or engaging in online activity connected with the school.

The policy applies to use of school devices, networks, accounts, internet access, email, online platforms and digital content, whether on or off site where the activity relates to the school or affects a member of its community. It should be read alongside the Child Protection and Safeguarding Policy, Social Media and AI Policy, Anti-Bullying Policy, Data Protection Policy and relevant staff and pupil acceptable use agreements.

2. Roles and responsibilities

- The Headteacher has overall responsibility for ensuring that online safety arrangements are in place, understood and reviewed.
- The Designated Safeguarding Lead (DSL) leads the response to online safety concerns involving safeguarding and ensures concerns are recorded and acted upon.
- All staff and volunteers must model safe and responsible use, follow this policy and report concerns promptly.
- Pupils are expected to follow the age-appropriate rules taught in school and seek help from an adult when something online makes them feel uncomfortable or unsafe.
- Parents and carers are encouraged to reinforce safe use at home, supervise children's online activity in an age-appropriate way and report concerns to the school.

3. Physical safety and care of equipment

- Electrical and digital equipment must be used in accordance with school health and safety arrangements and staff instructions.
- Pupils are taught to use equipment carefully, keep food and drink away from devices and adopt sensible posture and screen breaks.
- Users must treat school equipment with care and report damage, loss or faults to a member of staff.

- Only authorised personnel may install software, change device settings or connect unauthorised equipment to the school network.

4. Network, accounts and passwords

- Users must access school systems only through their own authorised account and must not use another person's login.
- Passwords must be kept confidential and must not be shared. Suspected compromise or unauthorised access must be reported immediately.
- Users must respect the privacy of other people's files and work. They must not access, alter, delete or share another user's information without permission.
- Files should be saved only in the appropriate school-approved locations and shared only with people who are authorised to access them.
- Users must not attempt to bypass security settings, filtering or monitoring, or download or install unauthorised software.
- Use of school networks and devices may be monitored in accordance with the school's policies and applicable law. Monitoring is used to support safeguarding, security and the proper use of systems.

5. Internet access, filtering and monitoring

Internet access at school is provided for learning and other authorised school purposes. The school uses filtering and monitoring arrangements intended to reduce the risk of access to harmful or inappropriate content. No filtering system can remove every risk, so supervision, education and prompt reporting remain essential.

- Pupils may use the internet only when a member of staff has given permission and in accordance with the activity's instructions.
- Pupils must use websites, apps and online services selected or approved by staff. They must not deliberately search for or access unsuitable, offensive or illegal material.
- If an unsuitable page, advert, message or image appears, pupils should stop, close it if safe to do so and tell a member of staff immediately. They should not investigate further or share it with others.
- Staff must use professional judgement, supervise pupils appropriately and report any suspected failure or weakness in filtering or monitoring arrangements to the Headteacher or DSL.
- Pupils' home internet use is primarily the responsibility of parents and carers. However, online activity outside school may be addressed by the school where it affects the safety or wellbeing of pupils, the orderly running of the school or members of the school community.

6. Email, messaging and online communication

- Pupils may use school-issued email or messaging accounts only when authorised by staff and for an agreed educational purpose.
- Pupils must communicate politely and appropriately, use approved recipients and never share personal details, passwords or confidential information.
- Pupils must not open unexpected attachments or links, respond to suspicious messages or communicate with unknown people. They should show the message to a trusted adult.
- Personal email, messaging or social media accounts must not be used by pupils for school activities unless specifically authorised by the Headteacher.
- Staff must use school-approved communication channels for school business and must not communicate privately with pupils through personal accounts.
- Staff should check recipients carefully before sending messages and take care when sharing attachments or information about pupils and families.

7. Digital images, video and audio

- The school may use photographs, video and audio recordings to support learning and celebrate school activities, in accordance with the school's image permissions and data protection arrangements.
- The school will consider the permissions and preferences recorded by parents and carers before publishing identifiable images. The school avoids publishing a child's full name alongside their image on public-facing platforms.
- Images and recordings must be stored securely and shared only for authorised purposes with appropriate access controls.
- Pupils must ask a member of staff before taking, copying, editing, moving or sharing images or recordings made in school.
- Staff and visitors must not take or publish images of pupils using personal devices unless this has been specifically authorised under school procedures.
- Images or recordings of pupils must not be uploaded to public AI tools or used to create animations, face swaps, voice clones or other manipulated media. Any exceptional proposed use requires prior approval from the Headteacher and the Data Protection Officer (DPO), as well as appropriate safeguarding and privacy checks.
- Parents and carers should follow school guidance at events and must not post images of other people's children without the relevant permission.

8. Artificial intelligence (AI) and emerging technologies

AI tools can generate or alter text, images, audio, video and other content. They may support learning when used carefully, but can also produce inaccurate information, biased material, fabricated sources and realistic-looking images or recordings that are not genuine.

- Pupils may use AI tools only when a member of staff has specifically authorised and is supervising the activity. Age restrictions and the terms of the service must be followed.
- Pupils must not enter personal information, photographs, names, contact details, passwords or confidential information about themselves or others into AI tools.
- Pupils must not use AI to impersonate, bully, threaten, embarrass or create misleading or harmful content about another person.
- Staff may use only school-approved AI tools for school work. Personal, confidential or special category data, including safeguarding, SEND, medical, assessment or family information, must not be entered into public or unapproved AI tools.
- Any proposed processing of personal data through an AI service must be discussed with the Headteacher and DPO before use. Staff must follow the school's data protection and information security arrangements.
- AI-generated content must be checked by a member of staff for accuracy, suitability, bias, copyright and potential harm before it is used with pupils or shared externally. Staff remain responsible for professional decisions and published material.
- AI must not replace professional judgement, safeguarding decisions, assessment decisions or direct communication with pupils and families.
- Where AI has materially contributed to a pupil's work, pupils should follow the teacher's instructions about acknowledging its use. AI-generated work must not be presented as entirely their own where this would be misleading.
- Staff and pupils must be alert to deepfakes, voice cloning, fake accounts and manipulated images. Suspected harmful or deceptive content must be reported to a member of staff or the DSL.

9. Online safety education

Online safety is taught as part of the curriculum and reinforced through everyday practice. Teaching is age-appropriate and may include:

- Keeping personal information, passwords and accounts secure.
- Recognising trustworthy and untrustworthy websites, messages, adverts and links.
- Understanding that online content may be inaccurate, misleading or designed to manipulate.
- Safe and respectful communication, including recognising and responding to cyberbullying.
- Knowing how to respond to upsetting content, unwanted contact or requests for personal information.
- Understanding age restrictions, privacy settings, digital footprints and the lasting impact of sharing content.
- Recognising AI-generated content, deepfakes and the importance of checking information and asking an adult for help.

Pupils are encouraged to speak to a trusted adult whenever they are worried about something they have seen, heard, received or created online. They will not be blamed for reporting a concern.

10. Cyberbullying and harmful online behaviour

Cyberbullying includes the use of digital communication to threaten, intimidate, humiliate, exclude or target another person. It may take place through messages, social media, online games, shared documents, images, video, audio or AI-generated content.

- All reports of online bullying will be taken seriously and dealt with in accordance with the school's Anti-Bullying Policy and safeguarding procedures.
- Pupils should not retaliate, forward harmful content or attempt to investigate the incident themselves. They should tell a trusted adult.
- Staff should report concerns promptly to the DSL or Headteacher and follow advice about recording and preserving evidence.
- The school may take action in relation to incidents outside school where they affect the safety or wellbeing of pupils, the orderly running of the school or members of the school community.

Where a concern may involve illegal content, exploitation, threats or immediate risk of harm, the DSL will consider appropriate referral to external agencies or the police. Staff should not download, copy or forward potentially illegal images; they should seek immediate advice from the DSL.

11. Mobile phones and personal devices

- Pupils must not have mobile phones or personal smart devices on their person during the school day. If a phone is brought to school with prior agreement, it must be handed to the school office for safekeeping for the duration of the day.
- Pupils must not use personal devices to take photographs, make recordings, access the internet or communicate during the school day.
- Staff must follow the school's arrangements for personal mobile phones and devices, particularly when supervising pupils. Personal devices must not be used to photograph or record pupils.
- Visitors and volunteers should follow staff instructions about the use of phones and recording equipment around pupils.

12. Other digital technologies

The same expectations apply to tablets, laptops, interactive displays, cameras, microphones, podcasting equipment, video-conferencing platforms, online learning environments, games and any new technology used in school.

- Online meetings and video calls must be arranged through approved platforms, supervised appropriately and used for an authorised school purpose.
- Recordings of lessons, meetings or online events must not be made or shared unless authorised.
- Staff should consider privacy, access, age suitability and safeguarding before introducing a new app, platform or digital service.

13. Copyright, plagiarism and digital content

- Users must respect copyright and intellectual property when using text, images, music, video, software and other online resources.
- Pupils should be taught to distinguish their own work from information or material taken from other sources and to acknowledge sources where appropriate.
- Pupils must not present another person's work, or AI-generated material, as their own where this would be misleading.
- Staff should check that content may lawfully be used and shared, particularly on the school website, newsletters, social media or other public platforms.
- AI-generated content is not automatically free of copyright or other legal restrictions. Staff must check the terms and suitability of any material before using it.

14. Data protection and information security

The school handles personal information in accordance with the UK GDPR, the Data Protection Act 2018 and the school's Data Protection Policy and privacy notices.

- Personal information must be accessed, used, stored and shared only when there is a legitimate school purpose and in accordance with staff responsibilities.
- Users must not share personal or confidential information through personal email accounts, public websites, social media or unapproved apps and AI tools.
- Devices and accounts must be protected with appropriate passwords and security measures. Devices containing school information must not be left unattended or made available to unauthorised people.
- Any suspected data breach, loss of a device, misdirected email, unauthorised disclosure or access to personal information must be reported immediately to the Headteacher and DPO in accordance with the school's data breach procedure.

15. Reporting concerns and responding to incidents

Any pupil, parent, member of staff, governor or volunteer who becomes aware of an online safety concern should report it promptly to the DSL or Headteacher. Staff must follow the school's safeguarding recording and reporting procedures.

- The school will consider the immediate safety and wellbeing of anyone affected and take proportionate steps to reduce further harm.
- Relevant information will be recorded and shared only with those who need to know.
- The school may review available school-system information in accordance with its monitoring, safeguarding and data protection arrangements.
- The school will consider whether parents or carers, the DPO, the local authority, the police or another agency should be informed.

- Staff must not promise absolute confidentiality where a safeguarding concern has been raised.

16. Breaches of this policy

A breach may result in action under the school's behaviour, safeguarding or disciplinary procedures, as appropriate. This may include restricting or withdrawing access to school systems, contacting parents or carers, or referring the matter to relevant agencies. Any response will be proportionate and take account of the circumstances and the age and understanding of the pupil concerned.

17. Review and related documents

This policy will be reviewed at least annually and sooner where changes in technology, guidance, safeguarding risks or school systems make this necessary. It should be read alongside the school's Child Protection and Safeguarding Policy, Social Media and AI Policy, Anti-Bullying Policy, Data Protection Policy, staff code of conduct and pupil acceptable use agreements.

Appendix 1: E-safety rules for Coral and Amber Classes

Think then Click

- We use the internet only when an adult is with us.
- We search the internet with an adult and use websites chosen by an adult.
- We click only on buttons or links when an adult has shown us what they do.
- We tell an adult if we see something that worries us or if we get lost online.
- We do not share our name, address, school details, photographs or other personal information online.
- We use kind words and ask an adult before sending or sharing anything.
- We do not use AI tools unless an adult is helping us.

Appendix 2: E-safety rules for Quartz and Jet Classes

- We ask permission before using the internet or a new website, app or AI tool.
- We use websites and services approved by an adult.
- We tell an adult straight away if we see anything that makes us uncomfortable, worried or confused.
- We close a page or stop an activity if we are unsure whether it is safe, and ask an adult for help.
- We only email or message people an adult has approved, and we are polite and respectful.
- We never share personal information, photographs, passwords or private details about ourselves or others.
- We do not arrange to meet anyone we have met online.
- We do not open unexpected emails, attachments or links.
- We do not create, share or forward hurtful messages, fake accounts, altered images, deepfakes or AI content about another person.
- We check information rather than assuming everything online or generated by AI is true.
- We tell an adult if someone asks us to keep an online interaction secret or makes us feel unsafe.

Policy administration

Policy owner	**Headteacher**
Reviewed	November 2026
Agreed by staff	November 2026
Approved by governors	November 2026
Next review	November 2027