

Cotgrave Candleby Lane School



E Safety and Online policy 2026 - 2027

Review date- September 2027

Policy Review: This policy has been developed in accordance with the current statutory safeguarding guidance, including *Keeping Children Safe in Education (KCSIE) 2025*, and will be reviewed following the publication of any updated statutory guidance or changes to relevant legislation to ensure continued compliance and best practice.

1. Aims

The aims of this policy are to:

- Safeguard and promote the welfare of all pupils, staff and members of the school community when using digital technologies.
- Create a culture in which technology is used safely, responsibly, respectfully and positively to support teaching, learning and communication.
- Ensure that online safety is recognised as an integral part of the school's wider safeguarding responsibilities.
- Minimise the risks associated with the use of technology, including those relating to content, contact, conduct and commerce.
- Provide a clear framework for preventing, identifying, reporting and responding to online safety concerns.
- Ensure that appropriate filtering and monitoring systems are in place to help protect pupils and staff while recognising that no technical solution can provide complete protection.
- Educate pupils to become safe, responsible and resilient digital citizens who can recognise and manage online risks both in and outside school.
- Promote positive online behaviour, respectful communication and responsible use of digital technologies.
- Support staff in fulfilling their safeguarding responsibilities through regular training and clear procedures.
- Work in partnership with parents and carers to promote safe and responsible technology use beyond the school environment.
- Ensure compliance with current safeguarding, data protection and cyber security legislation and statutory guidance.

Candleby Lane School recognises that technology plays a vital role in education and everyday life. While digital technologies provide significant opportunities for learning, communication and creativity, they also present safeguarding risks. The school is committed to providing a safe and secure digital environment where all members of the school community can use technology confidently, responsibly and safely.

2. Roles and Responsibilities

Safeguarding children in the digital environment is everyone's responsibility. Candleby Lane School recognises that online safety is an integral part of safeguarding and is embedded throughout the school's safeguarding culture, curriculum and everyday practice.

This policy applies to all members of the school community, including pupils, staff, governors, volunteers, contractors, visitors, parents/carers and anyone using the school's ICT systems or accessing school information.

All members of the school community are expected to act safely, responsibly and respectfully when using technology and to contribute to creating a positive and secure online environment.

All staff, governors, volunteers and regular visitors must read and sign the appropriate **Acceptable Use Agreement (AUA)** before accessing the school's ICT systems and must comply with this policy, the Staff Code of Conduct, Child Protection and Safeguarding Policy, Data Protection Policy and other relevant school policies.

The Governing Body has overall responsibility for ensuring that the school fulfils its statutory safeguarding duties in relation to online safety. Governors will ensure that appropriate policies, procedures, filtering and monitoring systems, staff training and resources are in place to safeguard pupils and staff from online risks.

The Headteacher has overall operational responsibility for implementing this policy and ensuring that online safety is effectively embedded across the school.

The **Designated Safeguarding Leads (DSL)** has strategic responsibility for online safety as part of the school's wider safeguarding arrangements. The DSL will:

- ensure online safety is embedded within the school's safeguarding procedures;
- respond appropriately to online safety concerns and incidents;
- ensure concerns are recorded and managed in line with the school's safeguarding procedures;
- work with external agencies where appropriate;
- ensure staff receive regular safeguarding and online safety updates; and
- monitor emerging online safeguarding risks and trends.

The **Computing Lead** is responsible for supporting the delivery of online safety education within the curriculum, promoting the safe and effective use of technology for teaching and learning, and working alongside the school's IT support provider and leadership team to ensure appropriate technical safeguards are maintained.

At the time of publication:

- **Computing Lead:** Louise Hemstock
- **Senior Leadership Team member and Designated Safeguarding Lead with strategic responsibility for Online Safety:** Iain Bly

All staff are responsible for:

- promoting safe, responsible and respectful use of technology;
- modelling positive digital behaviour;
- supervising pupils appropriately when using digital technologies;
- delivering online safety education where appropriate to their role;
- maintaining professional boundaries when using technology;
- reporting safeguarding or online safety concerns immediately to the Designated Safeguarding Lead;
- reporting concerns regarding the effectiveness of filtering or monitoring systems; and
- completing regular safeguarding and online safety training.

Pupils are expected to:

- use school technology safely, responsibly and respectfully;
- follow the school's Acceptable Use Agreement;
- protect their personal information and passwords;
- treat others with kindness and respect when communicating online;
- report anything online that makes them feel worried, uncomfortable or unsafe to a trusted adult; and
- understand that the school's network and devices may be monitored to help keep everyone safe.

Parents and carers play an essential role in promoting online safety. Candleby Lane School will work in partnership with parents and carers by:

- providing information and guidance to support safe technology use at home;
- promoting age-appropriate digital resilience and online safety awareness;
- informing parents and carers of significant online safety concerns where appropriate; and
- signposting families to trusted sources of online safety advice and support.

The school recognises that online safety is a shared responsibility and is committed to working collaboratively with pupils, families, staff, governors and external agencies to ensure that children can benefit from technology safely, responsibly and confidently.

Online Safety Risks

Candleby Lane School recognises that technology plays an essential role in education and everyday life. Whilst digital technologies provide significant opportunities for learning, communication and creativity, they also present safeguarding risks.

Online safety is an integral part of the school's safeguarding responsibilities. The school adopts a whole-school approach to identifying, managing and reducing online risks through education, appropriate technology, effective policies, staff training and partnership working with parents and carers.

In line with statutory guidance, the school recognises four broad categories of online risk:

4.1 Content Risks

Children may be exposed to illegal, harmful or inappropriate online content, including but not limited to:

- pornography and sexually explicit material;
- violent or distressing content;
- self-harm, suicide and eating disorder content;
- misinformation, disinformation and fake news;
- extremist, radicalising or terrorist material;
- racist, misogynistic, discriminatory or hateful content;
- content promoting criminal activity or harmful behaviours; and
- inappropriate use of artificial intelligence (AI) generated content.

Pupils are taught how to critically evaluate online information and recognise reliable and trustworthy sources.

4.2 Contact Risks

Children may experience harmful online interactions with others, including:

- online grooming;
- sexual exploitation;
- criminal exploitation, including county lines;
- coercion or manipulation;
- adults posing as children or young people;
- peer pressure;
- online harassment;
- unwanted contact from strangers; and
- commercial exploitation through advertising or scams.

The school teaches pupils how to recognise unsafe interactions, maintain healthy boundaries and seek support from trusted adults.

4.3 Conduct Risks

Children's own online behaviour can increase the risk of harm. This may include:

- cyberbullying;
- online harassment or abusive behaviour;
- sharing personal information;
- creating, sending or sharing inappropriate content;
- consensual and non-consensual sharing of nude and semi-nude images;
- misuse of social media, messaging platforms or online games;
- misuse of artificial intelligence (AI) tools;
- livestreaming risks; and
- behaviour that may negatively affect their wellbeing, reputation or future opportunities.

The school promotes respectful online behaviour and educates pupils about their digital footprint and responsibilities as digital citizens.

4.4 Commerce Risks

Children and adults may be exposed to financial risks online, including:

- phishing emails and messages;
- financial scams;
- identity theft;
- malicious software;
- inappropriate advertising;
- online gambling;
- subscription traps; and

- fraudulent online purchases.

The school promotes cyber awareness and encourages all members of the school community to report suspected scams or cyber security concerns immediately.

4.5 Emerging Technologies

The online environment continues to evolve rapidly. The school recognises that emerging technologies, including artificial intelligence (AI), social media platforms, livestreaming services and online gaming, present both opportunities and safeguarding risks.

Staff receive regular updates on emerging online risks and pupils are taught how to use new technologies safely, responsibly and ethically.

4.6 Responding to Online Safety Risks

Any concerns relating to online safety will be managed in accordance with the school's Child Protection and Safeguarding Policy and Behaviour Policy, where appropriate.

Incidents may include, but are not limited to:

- cyberbullying;
- online abuse or exploitation;
- inappropriate online content;
- sharing of nude or semi-nude images;
- harmful sexual behaviour facilitated through technology;
- concerns relating to radicalisation or extremism;
- misuse of school technology; and
- cyber security incidents.

Staff must report any online safety concern immediately to the Designated Safeguarding Lead (DSL), who will assess the concern and take appropriate action in line with statutory safeguarding guidance and local safeguarding procedures.

4. Online Safety Education

Online safety education is a fundamental part of the school's safeguarding and curriculum provision. Candleby Lane School recognises that children need to develop the knowledge, skills and behaviours to use technology safely, responsibly and respectfully both in school and beyond.

Online safety is taught through a progressive and age-appropriate curriculum, embedded across Computing, Personal, Social, Health and Economic (PSHE known as Healthy bodies Healthy minds in school) Education, Relationships Education, Health Education and other curriculum areas where appropriate.

The curriculum is informed by current statutory guidance, including the **Education for a Connected World Framework**, and aims to develop pupils' digital resilience and critical thinking.

Pupils will be taught to:

- use the internet and digital technologies safely, responsibly and respectfully;
- understand the benefits and risks associated with technology;
- protect their personal information, digital identity and privacy;
- recognise unsafe situations online and know how to respond appropriately;
- identify and report cyberbullying, online abuse and inappropriate content;
- understand healthy online relationships and respectful communication;
- critically evaluate online information, recognising misinformation, disinformation and fake news;
- understand the risks associated with social media, online gaming, messaging services and livestreaming;
- recognise online grooming, coercion and exploitation;
- understand the law and the risks relating to the creation, possession and sharing of nude and semi-nude images;
- use artificial intelligence (AI) tools safely, responsibly and ethically where appropriate; and
- understand how their online behaviour contributes to their digital footprint and future reputation.

Teaching will be adapted to meet the age, stage of development and individual needs of pupils, including those with SEND and other vulnerabilities.

Online safety messages are reinforced through assemblies, themed events, classroom discussions, curriculum enrichment opportunities and national awareness campaigns such as **Safer Internet Day**.

Staff Training

All staff receive online safety training as part of their safeguarding induction and regular safeguarding updates. Training is reviewed regularly to ensure staff remain aware of emerging technologies, current online risks and statutory safeguarding responsibilities.

Staff are expected to:

- model safe and responsible use of technology;
- maintain professional boundaries online;
- understand the procedures for reporting online safety concerns;
- recognise indicators of online abuse and exploitation; and
- support pupils in developing safe digital behaviours.

Working in Partnership with Parents and Carers

The school recognises that parents and carers play a vital role in promoting online safety.

Parents and carers will be supported through information, guidance and signposting to help them:

- understand current online risks;
- support safe technology use at home;
- reinforce positive online behaviours;
- understand the school's filtering and monitoring arrangements; and
- know where to seek advice if they have concerns about their child's online activity.

The school encourages open communication between home and school to promote a consistent approach to online safety.

5. Filtering and Monitoring

Candleby Lane School recognises that filtering and monitoring systems are an important part of safeguarding and are implemented in line with the Department for Education's **Filtering and Monitoring Standards for Schools and Colleges**.

Appropriate filtering and monitoring systems are in place on all school devices and networks to help protect pupils and staff from harmful or inappropriate online content while supporting effective teaching and learning.

The school recognises that filtering and monitoring systems form only one part of a wider safeguarding approach and cannot replace effective supervision, education and staff vigilance.

The school will ensure that:

- appropriate filtering systems are in place to block access to illegal, harmful and inappropriate content;
- monitoring systems are implemented to identify potential safeguarding concerns and inappropriate use of school technology;
- filtering and monitoring arrangements are reviewed regularly and at least annually;
- systems are appropriate to the age, needs and vulnerability of pupils;
- filtering does not unreasonably restrict access to educational resources;
- safeguarding concerns identified through monitoring are acted upon promptly in accordance with the Child Protection and Safeguarding Policy; and
- staff understand how to report concerns relating to the effectiveness of filtering and monitoring systems.

The Governing Body and Senior Leadership Team have strategic oversight of filtering and monitoring arrangements and ensure that appropriate roles and responsibilities are clearly defined.

The school's Academy Trust commissions **L.E.A.D. IT Services** to provide technical support, maintain filtering and monitoring systems and assist with regular reviews to ensure they remain effective and compliant with current guidance.

The school's filtering and monitoring arrangements are reviewed in partnership with the Academy Trust and IT provider to ensure they continue to meet the needs of the school community and reflect emerging safeguarding risks.

An annual online safety audit and risk assessment is completed by the school's Online Safety Lead and shared with the Designated Safeguarding Lead (DSL) team to inform future developments and improvements.

Where concerns are identified through filtering or monitoring systems, they will be assessed promptly by the appropriate members of staff. Where there is reason to believe a child may be at risk of harm, the concern will be managed in accordance with the school's safeguarding procedures and, where appropriate, external agencies will be involved.

The school will provide clear information to parents and carers about the school's filtering and monitoring arrangements and the measures in place to help keep children safe online. Parents and carers are encouraged to support safe technology use at home and to remain aware of the online platforms, services and devices their children access.

Filtering and monitoring arrangements are reviewed alongside the school's safeguarding risk assessments, including those undertaken as part of the Prevent Duty, cyber security arrangements and wider online safety provision, ensuring a coordinated and effective approach to safeguarding.

6. Managing Internet Access and ICT Systems

Candleby Lane School provides access to digital technologies and the internet to support teaching, learning and the effective operation of the school. Access is provided in a safe, secure and responsible manner that supports safeguarding and complies with relevant legislation.

All users of the school's ICT systems are expected to use technology responsibly and in accordance with the school's Acceptable Use Agreements, Staff Code of Conduct and Data Protection Policy.

6.1 Internet Access

The school provides pupils and staff with access to the internet for educational and professional purposes.

Internet access is designed to:

- enhance teaching and learning;
- support research and independent learning;
- develop pupils' digital literacy and online safety skills;
- enable effective communication and collaboration; and
- support the efficient management of the school.

Pupils will always be appropriately supervised when accessing online resources and staff will ensure that internet use supports planned learning objectives.

6.2 User Accounts and Network Access

The school maintains secure ICT systems through appropriate user management procedures.

The school will ensure that:

- all staff have individual user accounts;
- users are responsible for all activity carried out using their login credentials;
- passwords are kept secure and changed when required;
- accounts are removed or amended promptly when staff leave or change roles;
- access rights are proportionate to each user's role; and
- access to confidential information is restricted to authorised users.

Users must not share passwords or allow others to use their accounts.

6.3 Data Protection

The school processes personal data in accordance with the **UK General Data Protection Regulation (UK GDPR)** and the **Data Protection Act 2018**.

The school will ensure that:

- personal data is processed lawfully, fairly and transparently;
- confidential information is stored securely;
- access to personal information is restricted to authorised individuals;
- personal information is only shared where there is a lawful basis to do so; and
- all staff understand their responsibilities for protecting personal information.

Staff must report any actual or suspected personal data breach immediately in accordance with the school's Data Protection Policy.

6.4 Acceptable Use

All staff, governors, volunteers and visitors must read and sign the appropriate Acceptable Use Agreement before accessing school ICT systems.

Parents and carers will be informed of the school's expectations regarding pupils' safe use of technology and will be asked to provide appropriate permissions where required.

Failure to comply with the school's Acceptable Use Agreements may result in disciplinary action, withdrawal of ICT access or, where appropriate, referral to external agencies.

6.5 Monitoring ICT Use

The school reserves the right to monitor the use of its ICT systems, devices and networks where appropriate and lawful in order to:

- safeguard pupils and staff;
- investigate safeguarding concerns;
- protect school systems;
- maintain network security;
- investigate misuse of school technology; and
- ensure compliance with school policies.

Monitoring is carried out proportionately and in accordance with data protection legislation.

7. Cyber Security

The school recognises that cyber security is an essential element of safeguarding, business continuity and protecting personal data.

Appropriate technical and organisational measures are implemented to reduce the risk of cyber incidents and protect the confidentiality, integrity and availability of school information systems.

Working alongside the Academy Trust and **L.E.A.D. IT Services**, the school will ensure that appropriate cyber security measures are maintained.

These include:

- regularly updated antivirus and anti-malware protection;
- secure firewalls and network security controls;
- appropriate filtering and monitoring systems;
- software and operating system updates;
- secure password requirements and multi-factor authentication where appropriate;
- regular data backups;
- controlled user permissions;
- secure disposal of redundant equipment and data; and
- monitoring for suspicious network activity.

7.1 Email Security

School email accounts must only be used for professional purposes.

Staff will:

- use only approved school email accounts for school business;
- exercise caution when opening emails, attachments or links from unknown or unexpected sources;
- report suspicious emails, phishing attempts or potential cyber attacks immediately;
- not forward chain messages or unsolicited marketing emails using school systems; and
- ensure confidential information is shared securely and only where appropriate.

The school promotes awareness of phishing and social engineering attacks through regular staff training.

7.2 Remote and Flexible Working

Where staff work remotely or access school systems away from the school site, they must:

- use secure school-approved systems wherever possible;
- ensure devices are appropriately protected;
- maintain confidentiality when working in public or shared environments;
- avoid accessing sensitive information over unsecured public Wi-Fi;
- follow the school's Remote Working and Data Protection procedures; and
- ensure telephone numbers are withheld where personal devices are exceptionally used for work purposes, unless using school-approved communication systems.

7.3 Cyber Security Incidents

Any suspected cyber security incident, including phishing attacks, malware infections, unauthorised access, ransomware or data breaches, must be reported immediately to the Headteacher, Designated Safeguarding Lead where appropriate, and the Academy Trust's IT support provider.

The school will respond to cyber incidents in accordance with its Cyber Incident Response procedures, ensuring appropriate action is taken to:

- contain the incident;
- minimise disruption;
- protect personal data;
- investigate the cause;
- fulfil any statutory reporting requirements; and
- review systems and procedures to reduce future risk.

8. School Website, Social Media and Publishing Images

8.1 School Website

The school website is an important communication tool for pupils, parents/carers and the wider community. All published content will be accurate, appropriate and compliant with safeguarding and data protection legislation.

The Headteacher has overall editorial responsibility for the school's website and will ensure that published material:

- supports the school's values and ethos;
- is accurate, appropriate and regularly reviewed;
- complies with safeguarding, copyright and data protection legislation; and
- does not place pupils or staff at unnecessary risk.

Only the school's official contact details will be published. Personal contact information relating to pupils, staff or governors will never be published.

8.2 Publishing Pupils' Images and Work

The school celebrates pupils' achievements through displays, publications, newsletters, the school website and official social media channels.

To safeguard pupils:

- parental consent will be obtained before identifiable images or videos of pupils are published;
- pupils' full names will not be published alongside photographs unless there is a clear educational reason and appropriate consent has been obtained;
- images will be appropriate and respectful;
- photographs will not include information that could identify a child's location or personal details unnecessarily;
- staff will only use school-approved devices to capture photographs or videos of pupils; and
- images will be stored securely and deleted in accordance with the school's retention schedule.

Parents and carers will be informed of the school's procedures regarding photography and the publication of images.

8.3 Social Media

The school recognises that social media provides valuable opportunities for communication but also presents safeguarding and reputational risks.

The school maintains official social media accounts where appropriate to communicate with the school community.

Official accounts will:

- be managed by authorised members of staff;
- be regularly monitored;
- contain appropriate educational or community information;
- comply with safeguarding and data protection requirements; and
- follow the school's communication procedures.

Staff must not:

- communicate with pupils through personal social media accounts;
- accept or request personal social media connections with current pupils;
- discuss confidential school matters online; or
- publish material that could bring the school into disrepute.

Any concerns regarding social media misuse should be reported immediately to the Headteacher or Designated Safeguarding Lead, as appropriate.

9. Mobile Technologies and Emerging Technologies

Technology continues to evolve rapidly, and the school recognises both the educational benefits and safeguarding risks associated with emerging technologies.

Any new technology introduced into school will be subject to an appropriate risk assessment before use.

9.1 Mobile Phones and Personal Devices

The school has clear procedures regarding mobile phones and personal devices.

Pupils

Pupils who bring mobile phones to school must:

- hand them to their class teacher or the designated member of staff at the beginning of the school day;
- keep devices switched off unless authorised by a member of staff; and
- collect them at the end of the school day.

Pupils must not use personal devices during the school day unless specifically authorised for educational or medical purposes.

Staff

Staff are expected to use personal devices professionally and in accordance with the Staff Code of Conduct.

Staff must:

- avoid using personal mobile phones whilst supervising pupils except in emergencies;
- never use personal devices to photograph or record pupils;
- use school-approved devices wherever possible;
- maintain professional boundaries at all times; and
- ensure confidential information is not stored on personal devices unless authorised and appropriately secured.

9.2 Smart Technology and Wearable Devices

The school recognises that smart watches, wearable devices and internet-enabled technology are increasingly common.

Their use may be restricted where they could:

- compromise safeguarding;
- record images or audio without permission;
- disrupt learning;
- access inappropriate online content; or
- undermine examinations or assessments.

9.3 Artificial Intelligence (AI)

The school recognises that Artificial Intelligence (AI) is becoming increasingly common within education.

Where AI technologies are used, the school will ensure they are:

- appropriate for educational purposes;
- used safely, ethically and responsibly;
- compliant with data protection requirements;
- supervised by staff where appropriate; and
- used to support, rather than replace, teaching and learning.

Pupils will be taught to use AI critically and responsibly, understanding both its benefits and limitations.

9.4 Video Conferencing and Online Learning

Where video conferencing or online learning takes place, the school will ensure that:

- only approved platforms are used;
- sessions are appropriately supervised by members of staff;
- appropriate safeguarding measures are in place;
- participants understand expectations for behaviour; and
- personal information is protected.

10. Electronic Communication

Electronic communication supports effective teaching, learning and school administration.

All communication with pupils and parents/carers will take place using school-approved communication systems.

Staff must not use personal email accounts, messaging applications or personal social media to communicate with pupils.

Where online learning platforms are used, communication will remain professional, appropriate and capable of being monitored.

10.1 Email

School email accounts are provided for professional use only.

Staff will:

- use only approved school email accounts;
- check recipients carefully before sending emails;
- avoid sending confidential information unless appropriate security measures are used;
- exercise caution when opening links or attachments;
- report suspicious or phishing emails immediately; and
- comply with the school's Data Protection Policy.

Chain emails, spam and inappropriate communications must not be forwarded using school systems.

10.2 Approved Online Platforms

The school uses a range of approved digital learning platforms to support teaching and communication.

Any platform used by the school will be subject to appropriate safeguarding, privacy and data protection checks before implementation.

Communication through educational platforms will be moderated and monitored where appropriate.

11 Staff

All staff, governors, volunteers and regular visitors will:

- receive a copy of this Online Safety Policy or be directed to where it is published;
- read and sign the appropriate Acceptable Use Agreement before accessing school ICT systems;
- receive online safety training as part of safeguarding induction;
- receive regular safeguarding and online safety updates, including information on emerging technologies and online risks;
- understand that appropriate monitoring of school ICT systems may take place in accordance with school policies and data protection legislation; and
- understand their responsibility to report any online safety concern immediately to the Designated Safeguarding Lead.

Parents and Carers

The school will work in partnership with parents and carers by:

- making this policy available via the school website;
- providing information and guidance on online safety through newsletters, workshops, the school website and other communications;
- obtaining appropriate permissions relating to pupils' use of technology and publication of images;

- encouraging parents and carers to promote safe and responsible technology use at home; and
- signposting families to trusted online safety advice and support.

12. Related Policies

This policy should be read alongside the following school policies:

- Child Protection and Safeguarding Policy
- Staff Code of Conduct
- Behaviour Policy
- Anti-Bullying Policy
- Computing Policy
- Data Protection Policy
- Privacy Notices
- Acceptable Use Agreements
- Relationships, Sex and Health Education (RSHE) Policy
- Mobile Phone and Smart Device Policy (if separate)
- Remote Learning Policy (where applicable)
- Complaints Policy
- Whistleblowing Policy
- Prevent Risk Assessment
- Health and Safety Policy

13. Monitoring and Review

This policy will be reviewed at least annually by the Online Safety Lead, Designated Safeguarding Lead and Senior Leadership Team, and approved by the Governing Body.

The policy will also be reviewed:

- following changes to statutory guidance or legislation;
- following significant online safety incidents;
- following changes to the school's ICT infrastructure or filtering and monitoring arrangements; or
- where monitoring, audits or safeguarding reviews identify the need for improvement.

The effectiveness of this policy will be monitored through:

- safeguarding monitoring and audits;
- filtering and monitoring reviews;
- pupil, staff and parent feedback;
- incident reporting and trend analysis;
- curriculum evaluation; and
- governor safeguarding monitoring.

Appendix A – Acceptable Use Agreements (AUAs)

The following Acceptable Use Agreements form part of this policy and must be read alongside it:

- Staff, Governors, Volunteers and Visitors Acceptable Use Agreement
- Pupil Acceptable Use Agreement (EYFS/KS1)
- Pupil Acceptable Use Agreement (KS2)
- Parent/Carer Acceptable Use Agreement (where applicable)

These agreements are reviewed annually and signed before access is granted to school ICT systems.

Acceptable Use of the School's ICT Facilities and Internet



Agreement for Staff, Governors, Volunteers and Visitors

Name: _____

When using the school's ICT systems, devices, network, email, internet, cloud-based services or digital platforms, whether on school premises or remotely using a school device or authorised personal device, I agree that I will:

I will NOT:

- Access, attempt to access, download, create, store, share or distribute inappropriate material, including but not limited to material that is violent, extremist, discriminatory, illegal, abusive, sexually explicit or otherwise unsuitable.
- Use the school's ICT systems in any way that could damage the reputation of the school or bring the school into disrepute.
- Use school equipment or networks for unlawful, inappropriate or excessive personal use.
- Access social networking, messaging or gaming sites during working hours unless this forms part of my professional role or has been authorised by the Headteacher.
- Use inappropriate, offensive, discriminatory or unprofessional language when communicating electronically, including emails, messaging platforms or video conferencing.
- Install software, applications, browser extensions or connect hardware that has not been authorised by the school.
- Attempt to bypass the school's internet filtering, monitoring or security systems.
- Share my passwords, authentication codes or security credentials with anyone else or allow another person to use my account.
- Access, modify, delete or share information that I am not authorised to access.

- Share confidential or personal information relating to pupils, staff, governors or families unless this is necessary for my role and complies with the school's Data Protection Policy.
- Use personal email accounts or unauthorised cloud storage to store or transfer school information.
- Use unauthorised Artificial Intelligence (AI) tools to process confidential, personal or safeguarding information, or upload school documents to public AI platforms without approval.
- Photograph, record or share images or videos of pupils using personal devices unless specifically authorised in line with school policy.
- Promote or conduct private business activities using school ICT systems unless specifically authorised.

I WILL:

- Use all ICT systems professionally, responsibly and in accordance with school policies.
- Keep all passwords secure, use multi-factor authentication where provided, and report any suspected compromise immediately.
- Lock devices whenever they are left unattended and ensure devices used away from school are stored securely.
- Take reasonable precautions to protect school devices from theft, loss or damage.
- Ensure confidential information is only accessed where necessary and is stored and shared securely.
- Only use approved software, apps and cloud services for school business.
- Be vigilant for phishing emails, scams and cyber security threats and report anything suspicious immediately.
- Report any suspected data breach, cyber incident or loss of equipment to the ICT Manager and Data Protection Lead without delay.
- Ensure any personal devices used for school business comply with the school's Bring Your Own Device (BYOD) arrangements where applicable.
- Follow copyright and intellectual property laws when using digital resources.
- Ensure that all electronic communications with pupils and parents remain professional and take place only through approved school systems.

Safeguarding

I understand my safeguarding responsibilities when using technology and will:

- Immediately inform the Designated Safeguarding Lead (DSL) if I become aware of any online safety concern involving a pupil.
- Report any inappropriate online content, harmful material or concerning online behaviour involving pupils.
- Never communicate with pupils through personal social media accounts, personal messaging services or personal email addresses.
- Support pupils to use technology safely and responsibly in line with the school's Online Safety Policy.

Monitoring

I understand that:

- The school monitors and records the use of its ICT systems, internet access and email in accordance with its monitoring procedures and relevant legislation.
- There should be no expectation of privacy when using school ICT systems for school business.
- Monitoring may be undertaken to safeguard pupils and staff, maintain network security, investigate incidents and ensure compliance with school policies.

Data Protection

I understand that I am responsible for protecting personal data in accordance with:

- UK GDPR
- Data Protection Act 2018
- Data (Use and Access) Act 2025
- The school's Data Protection Policy and Information Security procedures

Cyber Security

I will:

- Complete any mandatory cyber security and online safety training required by the school.
- Follow the school's Cyber Security procedures.
- Immediately report any suspected cyber-attack, malware infection, ransomware, phishing attempt or suspicious activity.

Failure to comply with this agreement may result in disciplinary action, removal of ICT access, referral to relevant agencies where appropriate and, where applicable, criminal or civil proceedings.

I have read, understood and agree to comply with this Acceptable Use Agreement.

Name: _____

Role: _____

Signature: _____

Date: _____

Our School Computer and Internet Promise (KS1)



Name: _____

When I use computers, iPads and the internet at school, I promise that I will:

Be Safe - Only use the websites and apps my teacher tells me to use. - Tell an adult if I see something that worries, upsets or scares me. - Keep my passwords secret (unless my teacher asks for them). - Keep my personal information private, like my full name, address, phone number or passwords 	Be Kind - Use kind and respectful words when I am online. - Be polite to everyone. - Never send or share anything that could hurt someone else's feelings. 
Be Responsible - Look after school computers and iPads. - Only use my own login. - Ask an adult before I download or click on anything new. - Only take photos or videos if a teacher says I can.	Be Honest - Tell the truth if I make a mistake online. - Tell an adult straight away if something goes wrong. 
Use Technology Wisely - Remember that computers and AI tools can sometimes make mistakes. - Always ask my teacher if I am unsure about something I find online	

I know that my teachers help keep everyone safe by checking how the school computers and internet are used.

I promise to follow these rules every time I use technology at school.

Child's Signature: _____ Date: _____

Our Digital Learning Agreement (KS2)



Name: _____

Using technology is a privilege. I will use school computers, tablets, laptops and the internet safely, respectfully and responsibly.

I will:	I will NOT:
	
✓ Use technology to help me learn.	✗ Try to access websites or content that are not suitable for children.
✓ Only visit websites, apps and online services that my teacher has approved.	✗ Use another person's login or password.
✓ Keep my passwords private and only use my own account.	✗ Change computer settings or download apps without permission.
✓ Keep personal information safe, including my full name, address, phone number, passwords and other private details.	✗ Take or share photos, videos or recordings without permission.
✓ Be kind and respectful in all online communication.	✗ Send unkind, hurtful or inappropriate messages.
✓ Think carefully before I post, send or share anything online.	✗ Try to bypass school internet filters or security settings.
✓ Look after school equipment and tell an adult if something is broken or damaged.	
✓ Remember that anything I do online can leave a digital footprint.	
✓ Use AI tools only when my teacher says I can and never enter personal information into them.	

If something goes wrong...

I will tell a trusted adult straight away if:

- I see something that worries or upsets me.
- Someone is being unkind online.
- Someone asks me to keep an online secret.
- Someone asks for my personal information.
- I think someone has used my account.
- I accidentally click on something I shouldn't.

I understand that the school helps to keep everyone safe by monitoring how school technology is used.

I understand that if I do not follow this agreement, there may be consequences, including losing access to school technology for a period of time.

I promise to use technology safely, responsibly and respectfully.

Child's Signature: _____ Class: _____ Date: _____

Parent/Carer Acceptable Use Agreement

At Candleby Lane School, we believe that working in partnership with parents and carers is essential to helping children develop the knowledge, skills and confidence to use technology safely, responsibly and respectfully.

Technology plays an important role in children's education and everyday lives. We ask all parents and carers to support the school's Online Safety Policy by agreeing to the following expectations.

As a Parent/Carer, I will:

- Support my child in using the internet, digital technologies and social media safely, responsibly and respectfully.
- Encourage my child to follow the school's expectations for acceptable use of technology.
- Talk regularly with my child about their online activities, including the websites, games, apps and social media platforms they use.
- Encourage my child to tell me or another trusted adult if they see or experience anything online that makes them feel worried, upset or unsafe.
- Reinforce the importance of treating others with kindness and respect when communicating online.
- Encourage my child to keep personal information private and to use strong passwords.
- Support the school in promoting positive digital citizenship and responsible online behaviour.
- Ensure that any personal devices brought to school comply with the school's expectations and procedures.
- Use the school's communication systems appropriately and respectfully.
- Respect the privacy of other children, families and members of staff by not sharing photographs, videos or personal information without appropriate permission.
- Raise any concerns regarding online safety or inappropriate online behaviour with the school promptly.
- Work in partnership with the school to resolve any online safety concerns involving my child.

I understand that:

- The school uses filtering and monitoring systems on its network and devices to help safeguard pupils and staff.
- Internet access provided by the school is for educational purposes and is monitored where appropriate to help keep pupils safe.
- No filtering or monitoring system can completely eliminate online risks, and parents/carers continue to play an essential role in supporting safe technology use outside school.
- The school may investigate incidents involving misuse of technology where this impacts the safety or wellbeing of pupils, staff or the wider school community.
- Online behaviour outside school may be addressed by the school where it has a safeguarding impact or affects the welfare of pupils or staff.

- The school will manage online safety concerns in accordance with its Child Protection and Safeguarding Policy and other relevant policies.

Supporting Your Child at Home

Parents and carers are encouraged to:

- use parental controls where appropriate;
- supervise younger children when using internet-enabled devices;
- discuss age-appropriate screen time and healthy online habits;
- regularly review privacy settings on apps, games and social media;
- be aware of age ratings for games, apps and online platforms;
- encourage balanced use of technology alongside other activities; and
- access trusted online safety advice and guidance when needed.

Working Together

Candleby Lane School is committed to working in partnership with parents and carers to create a safe, positive and respectful digital environment for all children.

If you have any concerns regarding your child's online safety or wellbeing, please contact the school and speak to a member of the safeguarding team.

Parent/Carer Declaration

I have read and understood the Parent/Carer Acceptable Use Agreement.

I agree to support Candleby Lane School in promoting safe, responsible and respectful use of technology and the internet.

Parent/Carer Name: _____

Child's Name: _____

Class: _____

Signature: _____

Date: ____ / ____ / ____

Appendix B – Responding to Online Safety Incidents

All online safety concerns should be treated as safeguarding concerns where appropriate.

Staff should:

1. Stay calm and reassure the child.
2. Do not promise confidentiality.
3. Preserve any available evidence without forwarding or sharing illegal material.
4. Report the concern immediately to the Designated Safeguarding Lead (DSL).
5. Record the concern on the school's safeguarding recording system (e.g. CPOMS).
6. Follow the school's Child Protection and Safeguarding Policy.

The DSL will assess the concern and determine whether:

- parents/carers should be informed;
- external agencies should be contacted;
- a referral to Children's Social Care is required;
- police involvement is necessary;
- CEOP should be contacted; or
- additional support should be provided for the child.

Incidents involving the sharing of nude or semi-nude images must be managed in accordance with current UKCIS guidance and must not be viewed, copied or shared unnecessarily.

Appendix C – Useful Online Safety Resources

Reporting Concerns

- CEOP (Child Exploitation and Online Protection)
- Childline
- NSPCC
- Internet Watch Foundation (IWF)
- Action Fraud
- National Cyber Security Centre (NCSC)

Advice for Parents and Carers

- Internet Matters
- Childnet
- UK Safer Internet Centre
- Thinkuknow
- NSPCC Online Safety Hub

Cyber Security Advice

- National Cyber Security Centre (NCSC)
- Cyber Aware

Appendix D – Glossary

Term	Meaning
AI	Artificial Intelligence. Computer systems capable of generating content, analysing information or supporting decision making.
Cyberbullying	Bullying that takes place using digital technologies.
Digital Footprint	The information that exists online as a result of a person's activities.
Filtering	Systems used to restrict access to inappropriate online content.
Monitoring	Systems that identify potentially harmful or inappropriate online activity.
Phishing	Fraudulent attempts to obtain personal or financial information.
Livestreaming	Broadcasting live video over the internet.
Social Engineering	Attempts to manipulate people into revealing confidential information.
UKCIS	UK Council for Internet Safety

Appendix E – Legislation and Guidance

This policy has been developed with reference to:

Statutory Legislation

- Children Act 1989
- Children Act 2004
- Education Act 2002
- Counter-Terrorism and Security Act 2015 (Prevent Duty)
- Data Protection Act 2018
- UK General Data Protection Regulation (UK GDPR)
- Online Safety Act 2023
- Protection of Freedoms Act 2012
- Computer Misuse Act 1990
- Malicious Communications Act 1988
- Communications Act 2003

Department for Education Guidance

- Keeping Children Safe in Education (current edition)
- Working Together to Safeguard Children
- Teaching Online Safety in Schools
- Meeting Digital and Technology Standards in Schools and Colleges
- Filtering and Monitoring Standards for Schools and Colleges
- Searching, Screening and Confiscation
- Behaviour in Schools

Other National Guidance

- Education for a Connected World Framework (UKCIS)
- UKCIS – Sharing Nudes and Semi-Nudes: Advice for Education Settings
- UK Safer Internet Centre Guidance
- National Cyber Security Centre (NCSC) Guidance