



Burnt Ash
PRIMARY SCHOOL

Online Safety

Policy

This policy should be read with:

Child Protection & Safeguarding Policy

Behaviour for Learning Policy

Contents

1. Introduction and Overview

- Rationale
- Roles and responsibilities
- Communication
- Handling incidents/complaints
- Reviewing and Monitoring

2. Education and Curriculum

- Pupil online safety curriculum
- Staff and governor training
- Parent awareness and training

3. Expected Conduct and Incident Management

4. Managing the IT Infrastructure

- Filtering and monitoring
- Network management (user access, backup, curriculum and admin)
- Passwords policy
- E-mail
- School website
- Learning platform
- Social networking

5. Data Security

- Management Information System access
- Data transfer

6. Equipment and Digital Content

- Personal mobile phones and devices
- Digital images and video

Appendices:

A1: KS1 User Agreement

A2: KS2 User Agreement

A3: Acceptable Use Agreement (Staff, Volunteers and Governors)

A4: Acceptable Use Agreement including photo/video permission (Parents)

A5: Protocol for responding to online safety incidents

<http://www.lqfl.net/esafety/Pages/policies-acceptable-use.aspx> - handling infringements

<http://www.digitallyconfident.org/images/resources/first-line-information-support-HQ.pdf> - page 23 onwards

A6: Data security: Use of IT systems and Data transfer

Search and Confiscation guidance from DfE

<https://www.gov.uk/government/publications/searching-screening-and-confiscation>

1. Introduction and Overview

Rationale

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at Burnt Ash Primary School with respect to the use of IT-based technologies.
- Safeguard and protect the children and staff.
- Assist school staff working with children to work safely and responsibly with the Internet and other IT and communication technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use for the whole school community.
- Have clear structures to deal with online abuse & exploitation such as online bullying (linked to the safeguarding and behaviour policy).
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Minimise the risk of misplaced or malicious allegations made against adults who work with students.

Burnt Ash Primary School recognises that online safety is not a standalone safeguarding issue. Many safeguarding concerns now have an online element and online safety should be considered when responding to any safeguarding concern.

Risks may occur online, offline or through a combination of both. Staff should consider online safety when assessing concerns relating to child-on-child abuse, harmful sexual behaviour, exploitation, radicalisation, attendance, mental health, violence against women and girls, bullying and all other safeguarding matters.

The main areas of risk for our school community can be summarised as follows:

Content

- Exposure to illegal, inappropriate or harmful content such as pornography, disinformation, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism lifestyle websites and social media promoting harmful behaviours.
- Hate content including websites that promote hatefulness.
- Content validation: how to check authenticity and accuracy of online content.
- AI-generated harmful content, including deepfakes and manipulated media.
- Misogynistic content and material promoting violence against women and girls.
- Content promoting harmful online communities including incel ideology.

Contact

- Grooming (sexual exploitation, radicalisation etc.) – adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
- Subjected to harmful online interactions with other users, such as peer-to-peer pressure or commercial advertising.
- Online bullying in all forms.
- Identity theft (including through social media accounts) and sharing passwords.

- AI chatbots used for grooming.
- AI-assisted impersonation, deception or grooming.

Conduct

- Personal online behaviour that increases the likelihood of, or causes harm.
- Digital footprint and online reputation.
- Privacy issues, including disclosure of personal information.
- Health and well-being (amount of time spent online- internet or gaming).
- Sharing nudes and semi-nudes (sending and receiving of personally intimate images) and the sending or receiving of sexually inappropriate texts.
 - Upskirting (taking a picture under a person's clothing without their permission).
 - Copyright (little care or consideration for intellectual property and ownership).
 - Creating deepfakes.
 - Use of so-called 'nudification' apps which artificially create nude or semi-nude images of a person without their consent.
 - AI-generated bullying.
 - Image-based abuse, including sharing, creating or manipulating images without consent
 - Use of AI tools to create or share harmful content about others

Commerce

- Risks such as online gambling, inappropriate advertising, phishing and/or financial scams.
 - Financial exploitation facilitated through AI.

Emerging Online Risks

Staff at Burnt Ash Primary School are aware that safeguarding risks continue to evolve.

Emerging online risks may include:

- New forms of financial exploitation
- Child-on-parent abuse facilitated through technology
- Risks related to modern slavery and criminal exploitation
- Involvement with harmful online communities
- Links to 'Incel' ideology
- AI-enabled abuse
- Online radicalisation

Staff are not expected to be experts on all emerging risks but should remain professionally curious and report concerns in line with the school safeguarding procedures and log concerns on CPOMs where appropriate.

Scope (from SWGfL)

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

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students when they are off the school premises and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other online safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published policy.

Roles and responsibilities

Role	Key Responsibilities
Headteacher	• Must be adequately trained in off-line and online safeguarding, in-line with statutory guidance and relevant Local Safeguarding Partners guidance • To take overall responsibility for online safety provision • To take overall responsibility for data and data security (SIRO) • To ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements e.g. LGfL • To be responsible for ensuring that staff receive suitable training to carry out their online safety roles and to train other colleagues, as relevant • To be aware of procedures to be followed in the event of a serious e-Safety incident. • To receive regular monitoring reports from the Online Safety Leader • Is regularly updated in online safety issues and legislation, and be aware of the potential for serious child protection issues to 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 and use of social media • Liaise with the Local Authority and relevant agencies
DSL/s (supported by the Online Safety Leader/s)	• Takes lead responsibility for online safety in the school. • Ensures that staff understand this policy and that it is being implemented consistently throughout the school • Works with the Online Safety Leader and governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly • Takes the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks

Role	Key Responsibilities
	• Works with the Computing Leader and network technician to make sure the appropriate systems and processes are in place • Works with the Online Safety Leader, network technician and other staff, as necessary, to address any online safety issues or incidents • Ensures that any online safety incidents are logged and dealt with appropriately in line with this policy • Ensures updates and delivery of staff training on online safety • Undertakes annual risk assessments that consider and reflect the risks children face • Ensures regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively
Trustees/Online Safety trustee	• To ensure that the school follows all current online safety advice to keep the children and staff safe • To approve the Online Safety Policy • Review the effectiveness of the policy by receiving regular information about online safety incidents and monitoring reports from the Online Safety Leader. • To support the school in encouraging parents and the wider community to become engaged in online safety activities. • Ensure that all staff undergo safeguarding and child protection training, including online safety (which includes an understanding of the roles and responsibilities in relation to filtering and monitoring). • Ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks and regularly review their effectiveness. • Review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting those standards, which include: - Identifying and assigning roles and responsibilities to manage filtering and monitoring systems; - Reviewing filtering and monitoring provisions at least annually; - Blocking harmful and inappropriate content without unreasonably impacting teaching and learning; - Having effective monitoring strategies in place that meet their safeguarding needs.

Role	Key Responsibilities
Computing Curriculum Leader and Online Safety Leader	• Take day to day responsibility for online safety issues and a leading role in establishing and reviewing the school's online safety policy/documents • Promote an awareness and commitment to online safety throughout the school community • Ensure and oversee the delivery that online safety education is embedded within the curriculum • Liaise with school technical staff where appropriate • To communicate regularly with SLT to discuss current issues and review incident logs. • To ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident • To ensure that online safety incidents are logged as a safeguarding incident • Facilitate training and advice for all staff • To support the school in encouraging parents and the wider community to become engaged in online safety activities • To ensure that the school follows all current online safety advice to keep the children and staff safe • To ensure all LGfL services are managed on behalf of the school following data handling procedures as relevant
Network technician	• To report any online safety related issues that arises, to the Head Teacher • To ensure that users may only access the school's networks from school or at home through CISCO using properly enforced password protection. • To ensure that provision exists for misuse detection and malicious attack (e.g. keeping virus protection up to date) • To ensure the security of the school ICT system • To ensure that access controls/encryption exist to protect personal and sensitive information held on school-owned devices • The school's policy on web filtering is applied and updated on a regular basis. • that he/she keeps up to date with the school's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant • that the use of LGFL email is regularly monitored in order that any misuse/attempted misuse can be reported to the Head Teacher for investigation • To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster. • To keep up-to-date documentation of the school's e-security and technical procedures
SBM	• To ensure that the data they manage is accurate and up-to-date

Role	Key Responsibilities
	• Ensure best practice in information management. I.e. have appropriate access controls in place, that data is used, transferred and deleted in-line with data protection requirements. • The school must be registered with Information Commissioner
Teachers	• To embed online safety issues in all aspects of the curriculum and other school activities • To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extracurricular and extended school activities) • To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws.
LSAs	• To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extracurricular and extended school activities)
All staff (including LSAs and Teachers)	• To read, understand and help promote the school's online safety policies and guidance • To read, understand, sign and adhere to the school staff Acceptable Use Agreement • To be aware of online safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices • To report any suspected misuse or problem to the Head Teacher • To maintain an awareness of current e-Safety issues and guidance e.g. through CPD • To model safe, responsible and professional behaviours in their own use of technology • To ensure that any digital communications with pupils and their parents should be on a professional level and only through school based systems, never through personal mechanisms, e.g. personal email, text, mobile phones etc. • To understand that online safety forms part of safeguarding and should be considered whenever concerns are raised about a child's welfare. Exit strategy • At the end of the period of employment/volunteering to return any equipment or devices loaned by the school. This will include leaving PIN numbers, IDs and passwords to allow devices to be reset, or meeting with the head of ICT on the last day to log in and allow a factory reset.

Role	Key Responsibilities
Pupils	• Read, understand, sign and adhere to the Pupil Acceptable Use Policy (at KS1 parents/carers sign on behalf of the pupils) which is to be stored in their file in the office. • Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations • To understand the importance of reporting abuse, misuse or access to inappropriate materials • To know what action to take if they or someone they know feels worried or vulnerable when using online technology. • To know and understand school policy on cyber-bullying. • To understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's online safety policy covers their actions out of school, if related. • To take responsibility for learning about the benefits and risks of using the internet and other technologies safely both in school and at home
Parents/carers	• To support the school in promoting online safety and endorse the Parents' Acceptable Use Agreement which includes the pupils' use of the internet and the school's use of photographic and video images • To read, understand and promote the school Pupil Acceptable Use Agreement with their children • To consult with the school if they have any concerns about their children's use of technology
External groups including Parent groups	• Any external individual/organisation will sign an Acceptable Use Policy prior to using any equipment or the Internet within school

Communication:

The policy will be communicated to staff/pupils/community in the following ways:

- Policy to be posted on the school website, staffroom and will also be presented to all staff.
- Policy to be part of school induction pack for new staff.
- Regular updates and training on online safety for all staff.
- Acceptable use agreements discussed with staff and pupils at the start of each year and the signed document is to be stored in the appropriate files.

Handling Incidents/complaints:

- The school will take all reasonable precautions to ensure online safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.

- Staff and pupils are given information about infringements in use and possible consequences (if deemed necessary). These include:
 - Meeting with the Head Teacher/Online Safety Leader
 - Informing parents or carers
 - Removal of Internet or computer access for a period
 - Referral to LA/Police
- Online Safety lead acts as first point of contact for any incident. Any complaint about staff misuse is referred to the Head teacher (unless the concern is about the Headteacher, in which case the incident is referred to the Chair of Governors and LADO).

Burnt Ash Primary School recognises the following types of incidents and lays out it's approach in responding.

Online Sexual Harassment

Definition: Unwanted sexual comments, jokes, or images shared online, including via social media, messaging apps, or gaming platforms.

School Response:

- Treat all reports seriously and respond promptly in line with safeguarding procedures.
- Ensure the Designated Safeguarding Lead (DSL) is informed immediately.
- Record incidents on the school's safeguarding system (CPOMS) and assess risk to the child.
- Provide support to the pupil affected, including emotional wellbeing and parental engagement.
- Consequences issued (if necessary) following the school's behaviour policy.
- Educate pupils through age-appropriate **RSHE curriculum** about respectful online behaviour and consent.
- Report to external agencies (police/children's social care) if the behaviour meets the harm threshold under KCSIE Part Five.

Violence Against Women and Girls (VAWG)

Definition: Burnt Ash Primary School recognises that harmful attitudes towards women and girls can develop during childhood and may be reinforced through online content and online communities. Violence Against Women and Girls (VAWG) includes behaviours, attitudes or content that promote, normalise or encourage misogyny, gender-based abuse, sexual harassment, coercion or violence towards women and girls.

This may include:

- misogynistic comments
- sexist language
- exposure to harmful influencers
- online harassment
- sharing degrading content
- gender-based abuse

School Response:

- Reports of misogyny, sexist behaviour, gender-based abuse or online harassment will be treated seriously and responded to in line with our safeguarding and behaviour policy.
- Children will be educated about respectful relationships, equality, consent and healthy attitudes towards others through PSHE and the wider school curriculum and culture.
- Incidents will be recorded and monitored where appropriate to identify patterns or emerging concerns.
- Inform parents and provide guidance regarding filtering content at home.

Online Harmful Sexual Behaviour

Definition: Sexualised actions online that are developmentally inappropriate, coercive, or abusive (e.g., sharing explicit images, sexualised chat).

School Response:

- Use the KCSIE guidance to assess behaviour.
- Intervene early with safeguarding and pastoral support; consider referrals to specialist services.
- Educate pupils on healthy relationships and digital boundaries through RSHE.
- Monitor and review filtering and monitoring systems to prevent access to harmful content.
- Inform parents and provide guidance on managing online risks at home.

Upskirting

Definition: Taking a photo or video under someone's clothing without consent, including sharing such images online. This is a criminal offence under the Voyeurism Act 2019.

School Response:

- Treat as a serious safeguarding and criminal matter; report to the DSL & police immediately.
- Secure and preserve any evidence (e.g., device, screenshots) following KCSIE advice.
- Support the pupil affected and involve parents sensitively.
- Apply appropriate support for the pupil who instigated incident and follow police advice.
- Reinforce education on privacy, respect, and consent in RSHE lessons.

Image-Based Abuse

Definition: Image-based abuse refers to the creation, sharing, manipulation or threatened sharing of images without consent where the intent is to cause distress, fear or harm.

This may include:

- Sharing intimate images
- Altered images
- Deepfakes
- AI-generated images
- 'Nudification' technology
- Threats to share images

School Response:

- Inform the DSL immediately
- Avoid viewing or forwarding images unnecessarily (in line with our guidance)

- Not to request pupils to share images
- Ensure evidence is preserved where appropriate
- Record the incident on CPOMS

The DSL will then determine, in conversation with staff, whether external agencies including Children's Social Care or the Police should be involved.

Sexualised Bullying

Definition: Bullying that includes sexual language, gestures, or sharing sexual content online.

School Response:

- Addressed in line with the Child protection and Safeguarding Policy.
- Investigate promptly; involve the DSL and record actions.
- Provide restorative approaches where appropriate, alongside sanctions.
- Offer counselling or wellbeing support for pupil affected.
- Embed preventative education in RSHE and online safety lessons.

Online misinformation and disinformation

Definition: Misinformation can be defined as false content shared without harmful intent. Disinformation can be defined as false or manipulated content shared deliberately to cause harm or mislead. This includes conspiracy theories, extremist narratives, health-related misinformation, AI-generated deepfakes, altered images or videos, and misleading "fake news" posts shared on social media, gaming platforms or messaging apps.

School Response:

- Teach pupils how to question, verify and critically evaluate information they encounter online.
- Provide staff with training so they can recognise when misinformation or disinformation is influencing a pupil's behaviour, wellbeing or beliefs and understand how to respond.
- Treat any incident where misinformation causes fear, distress, harmful behaviour, or impacts safeguarding as a safeguarding concern and record it on CPOMS.
- Provide parents with guidance on helping children recognise misleading content at home (through workshops and talks at the end of family assemblies).
- Work with external agencies where misinformation relates to radicalisation, extremism, online challenges or other harmful content in line with our Safeguarding policy.

Mitigating Risk from Unsupervised Access on Personal Devices

Burnt Ash Primary School reduces risks from pupils using personal devices by enforcing clear acceptable use policies and maintaining robust filtering and monitoring systems. Staff are regularly informed as to how to respond promptly to alerts and understand how to report necessary information using the school's safeguarding reporting procedure (CPOMS). The school regularly educates pupils on safe online behaviour and works closely with parents to promote responsible device use at home. Risk assessments consider age-specific issues such as exposure to harmful content, grooming, viral challenges, and the approach is reviewed regularly to keep staff updated.

Managing Viral Trends

To address viral trends that may encourage unsafe or disruptive behaviour, Burnt Ash Primary School combines proactive education with effective safeguarding responses. Pupils are taught digital literacy and critical thinking to help them recognise and resist harmful online influences. Staff monitor emerging trends through regular updates from the Online Safety lead and Pastoral Lead to assist them to act quickly if risks arise, following safeguarding procedures and involving parents where necessary. Clear communication and preventative education reduce the likelihood of harm and ensure pupils understand the impact of online trends.

Accessing a Child's Personal Device

The Online Safety Lead or DSL may access a pupil's personal device (e.g., mobile phone or tablet) without the child's or parents' consent when there are reasonable grounds to suspect that the device contains material that poses a safeguarding risk or is linked to prohibited items or harmful behaviour. This is permitted under:

- **Education Act 1996 and DfE guidance on Searching, Screening and Confiscation**, which gives headteachers and authorised staff statutory power to search a pupil or their possessions without consent if there is reasonable suspicion of prohibited or harmful content.
- **Keeping Children Safe in Education (KCSIE)**, which requires staff to act in the best interests of the child and prioritise safeguarding over consent where necessary. [\[gov.uk\]](https://www.gov.uk)
- **UK GDPR and Data Protection Act 2018**, which allow processing of personal data without consent when it is necessary for compliance with a legal obligation or to protect vital interests (safeguarding). [\[gov.uk\]](https://www.gov.uk)

Key safeguards:

- Searches must be proportionate, justified, and documented, with two staff present where possible (This should be the Online Safety Leader/ a DSL/ a member of SLT).
- Only relevant material should be accessed; unnecessary intrusion into private content must be avoided.
- The action must be recorded in the safeguarding log (CPOMS) and reported to the Designated Safeguarding Lead (DSL).
- Parents/carers should be informed after the search, unless doing so would place the child at further risk.

Police Thresholds for Online Incidents

Burnt Ash Primary School follows the National Police Chiefs' Council (NPCC) *When to Call the Police* guidance for schools and colleges. The school will not conduct detailed internal investigations into incidents that may constitute criminal offences. Staff will establish basic facts only and then refer immediately to the DSL for decision-making.

The school will contact the police when any online incident involves:

- Sexual offences or harmful sexual behaviour
- Threats of serious violence or severe harm
- Hate crimes or targeted harassment
- Criminal online behaviour
- Any incident where a child is at immediate risk of harm

The school and staff members will not:

- View indecent images of children (including nudes/semi-nudes)
- Ask pupils to forward, share or delete images
- Attempt to identify or question alleged perpetrators beyond basic fact-finding
- Attempt to “resolve” criminal behaviour internally

DSL responsibilities:

The DSL will:

- Make the decision about contacting police and who will be the single point of contact
- Record the rationale on CPOMS
- Liaise with MASH and police
- Ensure the child is supported throughout
- Inform parents unless this puts the child at risk

Reviewing and Monitoring

- The online safety policy will be reviewed annually as part of the school's monitoring cycle or sooner if new guidelines are released or when any significant changes occur with regard to the technologies in use within the school.
- The school's DSL and Online Safety Leader will be responsible for document ownership, review and updates.
- There is widespread ownership of the policy and it has been agreed by the SLT and approved by Trustees. All amendments to the school online safety policy will be disseminated to all members of staff.
- In line with the Online Safety Act 2023 (in force from 25 July 2025), Burnt Ash Primary School ensures that all online platforms used or recommended within the school comply with statutory requirements relating to age-verification, harmful content, and reporting mechanisms. Staff and pupils are made aware that service providers must enforce age-verification before access to harmful content (including pornography, self-harm, suicide or eating disorder material). The school will only use platforms and search tools that meet Ofcom's updated codes of practice, including requirements for risk assessments, transparency, and accountability. The effectiveness of these systems will be reviewed annually as part of our safeguarding and online safety monitoring processes.

2. Education and Curriculum

Pupil online safety curriculum

This school:

- Has a clear, progressive online safety education programme as part of the Computing curriculum/PSHE curriculum. It is built on LGfL (Project EVOLVE) e-safeguarding framework for EYFS to Y6/national guidance along with other schemes deemed appropriate. This covers a range of skills and behaviours appropriate to their age and experience, including:
 - to STOP and THINK before they CLICK
 - to develop a range of strategies to evaluate and verify information before accepting its accuracy;
 - to be aware that the author of a web site/page may have a particular bias or purpose and to develop skills to recognise what that may be;

- to know how to narrow down or refine a search;
 - [for older pupils] to understand how search engines work and to understand that this affects the results they see at the top of the listings;
 - to understand acceptable behaviour when using an online environment / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private;
 - to understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
 - to understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments;
 - to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings;
 - to understand why they must not post pictures or videos of others without their permission;
 - to know not to download any files – such as music files - without permission;
 - to have strategies for dealing with receipt of inappropriate materials;
 - [for older pupils] to understand why and how some people will exploit and 'groom' young people for sexual reasons
 - To know how to identify and critically evaluate online misinformation and disinformation, including recognising bias, checking sources, and understanding how false information can be used to manipulate or harm.
 - to understand the impact of cyberbullying, sexting and trolling and know how to seek help if they are affected by any form of online bullying.
 - to know how to report any abuse including cyberbullying; and how to seek help if they experience problems when using the Internet and related technologies, i.e. parent or carer, teacher or trusted staff member, or an organisation such as ChildLine or the CLICK CEOP button.
- Will remind students about their responsibilities through the pupil Acceptable Use Agreement(s)
 - Ensures staff are aware of their responsibility to model safe and responsible behaviour in their own use of technology, e.g. use of passwords, logging-off, use of content, research skills, copyright;
 - Ensures that staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright/intellectual property rights;
 - Ensures pupils only use school-approved systems and publish within appropriately secure/age-appropriate environments.
 - Ensures that staff and pupils understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include, risks in pop- ups; buying on-line; on-line gaming / gambling;

Staff and governor training

This school:

- Makes regular training available to staff on online safety issues and the school's online safety education program; at least annually but more often if the need is felt to arise.
- Provides regular updates via email and staff briefings as required to continue to provide the relevant skills and knowledge for staff and governors to safeguard children effectively.
- Provides, as part of the induction process, all new staff [including those on university/college placement and work experience] with information and guidance on the Online Safety Policy and the school's Acceptable Use Agreements.
- Provides resources for staff to use throughout the year to allow them to keep up to date with new Online Safety issues and educate themselves on areas they feel less confident on.
- Training will cover recognising when misinformation or disinformation is impacting pupils' views, behaviours or wellbeing, and strategies for addressing this sensitively.

Parent awareness and training

This school:

- runs a rolling programme of online safety advice, guidance and training for parents including:
 - Information leaflets sent home with the children and at parent's evenings;
 - Demonstrations and practical sessions held at school;
 - Suggestions for safe Internet use at home
 - Weekly briefings during Family Assembly time to reflect the key online safety message of that term including helping children recognise false or misleading online content and in reporting harmful material
 -

3. Expected Conduct and Incident management

Expected conduct

In this school, all users:

- Are responsible for using the school IT and communication systems in accordance with the relevant Acceptable Use Agreements
- Need to understand the importance of misuse or access to inappropriate materials and are aware of the consequences
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school
- Will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand-held devices, including smart-watches. They should also know and understand school policies on the taking images and on online bullying

Staff

- Understand that technology is a significant component in many safeguarding and wellbeing issues.
- Are responsible for reading the school's online safety policy and using the school ICT systems accordingly, including the use of mobile phones, smart-watches and hand-held devices.

- Are to be vigilant in the supervision of younger children, and use common-sense strategies where older pupils have more flexible access;
- Know to take professional, reasonable precautions when working with pupils, previewing websites before use;

Parents/Carers

- Should provide consent for pupils to use the Internet, as well as other technologies, as part of the online safety acceptable use agreement form at time of their child's entry to the school
- Should know and understand what the 'rules of appropriate use' are and what sanctions result from misuse

4.Managing the IT infrastructure

Filtering and Monitoring

The DSL has strategic oversight of the school's filtering and monitoring arrangements. The DSL will:

- Understand how the filtering and monitoring systems work, what they block and their limitations
- Monitor filtering and monitoring reports, identify safeguarding concerns and act on them
- Ensure online safety risks identified through monitoring are recorded on CPOMS and addressed through safeguarding procedures
- Work with technical staff (ATS) before any changes are made to filtering rules to ensure changes do not weaken pupil safety

Online Safety Lead / Computing Lead

- Supports the DSL by reviewing monitoring alerts and reports
- Advises on pupil risk trends (e.g. search terms, repeated attempts to access certain categories)
- Helps ensure the filtering and monitoring systems meet teaching and safeguarding needs

Network Technician

- Manages the day-to-day operation of filtering and monitoring systems
- Ensures filtering systems meet DfE standards, are functioning correctly and receive updates
- Logs all changes or requests to change filtering settings
- Alerts the DSL immediately if a technical issue results in reduced filtering or monitoring

Trustees

- Receive an annual report evaluating the effectiveness of the filtering and monitoring arrangements.
- Ensure filtering and monitoring remain appropriate and proportionate.

Annual Review

The school conducts a formal annual filtering and monitoring review, led by the DSL, Online Safety Lead and Network Technician. The review includes:

- Testing the effectiveness of filtering categories and blocks
- Evaluation of monitoring alerts and trends
- Review of staff understanding and training needs
- Identification of new risks or technologies used by pupils
- Confirmation that systems meet the latest DfE and KCSIE requirements

The outcomes are reported to Trustees and stored within safeguarding records.

Staff Understanding

All staff are trained so they understand:

- What the filtering system does and does not block
- How pupils may attempt to bypass filters using mobile data or VPNs
- How monitoring works and what types of behaviour or risks it alerts the school to
- How to escalate concerns raised through monitoring systems
- Their responsibility to report any filtering failures immediately to the DSL or Network Technician

This ensures staff can take appropriate safeguarding action when necessary.

Risk Assessment Prior to Changes

Any proposed changes to the filtering or monitoring systems must be subject to a formal safeguarding risk assessment, led by the DSL. This includes:

- Reviewing the purpose of the change
- Assessing whether the change introduces new risks
- Determining what supervision or restrictions may need adjusting
- Recording the rationale for the decision

No changes will be made to filtering settings unless the DSL has approved them following this risk assessment.

Monitoring Processes

The school uses LGfL to monitor pupil activity on school devices. Monitoring alerts are:

- Reviewed regularly by the DSL/Online Safety Lead
- Logged on CPOMS when safeguarding concerns arise
- Used to inform early help, pastoral support or safeguarding referrals in line with our Safeguarding policy

Monitoring is both proactive (through automated alerts) and reactive (through staff escalation and reports).

LGfL

LGfL's role is to provide:

- Educational filtered secure broadband connectivity through the LGfL and so connects to the 'private' National Education Network;
- LGfL Net Sweeper filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc. All changes to the filtering policy is logged and only available to staff with the approved 'web filtering management' status;
- Ensured network health through use of anti-virus software
- LGfL approved systems, including CISCO, to securely access the network system remotely to access personal level data off-site
- Blocks all chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform;
- Only unblock other external social networking sites for specific purposes
- Block pupil access to music download or shopping sites – except those approved for educational purposes at a regional or national level, such as Audio Network
- Block inappropriate games and websites on computers and iPads.

Network management (user access, backup)

This school:

- Uses individual, audited log-ins for all staff - the LGfL USO system;
- Ensures the Systems Administrator/network manager is up-to-date with LGfL services and policies/requires the Technical Support Provider to be up-to-date with LGfL services and policies;
- Has regular back-up of school data (teacher share and SLT drive);
- Storage of all data within the school will conform to UK data protection requirements;

To ensure the network is used safely, this school:

- Ensures staff read and sign that they have understood the school's Online Safety Policy. Following this, they are set-up with Internet, email access and network access. Online access to service is through a unique, audited username and password. This is used to log in to LGFL mail but is a different username/password than the one used to access the school's system.
- Has set-up the network with a shared work area for pupils (pupil share) and one for staff (teacher share). Staff and pupils are shown how to save work and access work from these areas;
- Has integrated curriculum and administration networks, but access to the Management Information System is set-up so as to ensure staff users can only access modules related to their role; e.g. SLT accessing SLT drive, Rainbow room accessing Pastoral drive;
- Requires all users to log off or 'lock' their laptops when they have finished working or are leaving the computer unattended for more than 10 minutes at time e.g. break times/lunch times;

- Ensures all equipment owned by the school and/or connected to the network has up to date virus protection;
- Makes clear that staff are responsible for ensuring that all equipment that goes home has the anti-virus and spyware software maintained up-to-date and the school provides them with a solution to do so;
- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used primarily to support their professional responsibilities.
- Does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is restricted and is only through approved systems; e.g. technical support or MIS Support, our Education Welfare Officers accessing attendance data on specific children
- All computer equipment is installed professionally and meets health and safety standards;
- Reviews the school ICT systems regularly with regard to health and safety and security.

Password policy

- This school makes it clear that staff and pupils must always keep their passwords private, must not share with others; if a password is compromised the school should be notified immediately. This includes passwords for education sites such as Mathletics, Accelerated reader, Padlet etc.
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password to their LGFL email account and to the school's network private.

E-mail

This school

- Provides staff with an email account for their professional use, (Microsoft Outlook) and makes clear personal email should be through a separate account;
- Does not publish personal e-mail addresses of pupils or staff on the school website. Instead using the office's main account admin@burntashprimary.co.uk for main correspondences.
- Will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law.
- Will ensure that email accounts are maintained and up to date.
- Knows that spam, phishing and virus attachments can make emails dangerous. We use a number of LGfL-provided technologies to help protect users and systems in the school, including direct email filtering for viruses, Trojans, pornography, phishing and inappropriate language. Finally, and in support of these, LGfL WebScreen2 filtering monitors and protects our Internet access to the World Wide Web.

Pupils:

- Pupils are taught about the online safety around using e-mail both in school and at home. Including:
 - not to give out their e-mail address unless it is part of a school managed project or to someone they know and trust and is approved by their teacher or parent/carer;

- that an e-mail is a form of publishing where the message should be clear, short and concise;
 - that any e-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper;
 - they must not reveal private details of themselves or others in e-mail, such as address, telephone number, etc.;
 - to 'Stop and Think Before They Click' and not open attachments unless sure the source is safe;
 - that they should think carefully before sending any attachments;
 - that they must immediately tell a teacher/responsible adult if they receive an e-mail which makes them feel uncomfortable, is offensive or bullying in nature;
 - not to respond to malicious or threatening messages;
 - not to delete malicious or threatening e-mails, but to keep them as evidence of bullying;
 - not to arrange to meet anyone they meet through e-mail without having discussed with an adult and taking a responsible adult with them;
 - that forwarding 'chain' e-mail letters is not permitted.
- Pupils sign the school Agreement Form to say they have read and understood the online safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

Staff:

- Staff only use Microsoft Outlook e-mail systems for professional purposes.
- All staff sign our acceptable use form to say they have read and understood the online safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

School website

- The Headteacher, supported by the Governing body, takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;
- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status;
- Uploading of information is restricted to our website authorisers.
- The school web site complies with the statutory DfE guidelines for publications;
- The point of contact on the web site is the school address, telephone number and we use a general email contact address, e.g. admin@burntashprimary.co.uk. Individual e-mail identities will not be published;
- Photographs published on the web do not have full names attached;
- We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website;

Social networking

Staff, Volunteers and Contractors

- Staff are instructed to always keep professional and private communication separate.

- The school's Facebook and Instagram account will be maintained and access only by the Assistant Headteacher and Computing Lead and is used for school related news only.
- Photographs or videos posted via the school's Facebook and Instagram account will not be face on, identifiable images and do not have names linked to them.

School staff will ensure that in private use:

- No reference should be made in social media to pupils (current or past), parents/carers or school staff
- School staff should not be 'friends' with any pupil/student or student's parents.
- They do not engage in online discussion on personal matters relating to members of the school community
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Pupils:

- Are taught about social networking, acceptable behaviours and how to report misuse, intimidation or abuse through our online safety curriculum work.
- Are taught about the safe use of social media, including how privacy and security settings will help to keep them safe.
- Students are required to sign and follow our age appropriate pupil Acceptable Use Agreement.

CCTV

- We have CCTV in the school as part of our site surveillance for staff and student safety. The use of CCTV is signposted in the school. We will not reveal any recordings without appropriate permission. Staff only view the CCTV with permission of the headteacher or deputy.

5. Data security: Management Information System access and Data transfer

Strategic and operational practices

At this school:

- The Head Teacher is the Senior Information Risk Officer (SIRO).
- Staff are clear who the key contact(s) for key school information (the Information Asset Owners) are.
- We ensure staff know who to report any incidents to and how, if data protection may have been compromised.
- All staff are DBS checked and records are held in a single central record
- We ask staff to undertake at least yearly house-keeping to review, remove and destroy any digital materials and documents which need no longer be stored.

Technical Solutions

- Staff have secure areas on the network to store sensitive files (teacher share/pastoral drive/SLT drive)

- We require staff to log-out/lock their systems when leaving their computer.
- All servers are in lockable locations and managed by DBS-checked staff.
- Disposal of any equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website.

6. Equipment and Digital Content

Mobile Phone Expectations

- Burnt Ash Primary School follows the Department for Education guidance that schools should be mobile phone free environments by default.
- All staff mobile phones should be stored securely and out of sight during the school day. Staff should only access personal devices during designated break periods in the staffroom or in offices away from children.
- In extreme circumstances, exceptions are permitted but staff/ parents need to clearly communicate this to the DSL/ Deputy DSL and must be granted explicit permission. This is to safeguard both children and staff themselves.
- The school recognises that mobile devices can increase safeguarding risks including cyberbullying, image sharing, online harassment and access to harmful content.

Mobile Devices (Mobile phones, tablets and other mobile devices)

- Mobile devices brought into school are entirely at the staff member, students, parents or visitors own risk. The school accepts no responsibility for the loss, theft or damage of any phone or hand-held device brought into school.
- The school reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying. Staff mobiles or hand-held devices may be searched at any time as part of routine monitoring.
- Mobile phones and personally-owned devices (including smart-watches) should not be used during the school day, except during designated break times. During these times, devices should only be used in the staffroom or office space/classroom where no children are present.

Children's use of personal devices

- The school strongly advises that children should not bring mobile phones into school, although the school accepts that there may be circumstances in which a parent wishes their child to have a mobile phone for their own safety, such as year 5 and 6 children walking to/from school alone. Children must ensure the device is switched off on arrival at the school site and must hand the device directly to the school office on arrival. Devices will be stored securely and returned at the end of the school day. Parents must complete a parental consent form on Arbor if their child will be bringing a device into school.
- If a child breaches the school policy by not handing it in, then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents or carers in accordance with the school policy.

- If contact needs to be made with a parent, this is managed via the school office. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.
- Children should protect their phone numbers by only giving them to trusted friends and family members. Students will be instructed in safe and appropriate use of mobile phones and personally owned devices and will be made aware of boundaries and consequences.
- Children are not allowed to have smart watches in school which have internet connection (unless specifically agreed with the headteacher on medical grounds). If these are brought in they are held in a secure place in the school office. They will be released to parents or carers in accordance with the school policy.
- Children are not allowed to take mobile phones or smart watches on residential trips (unless specifically agreed with the headteacher on medical grounds). If a child is found to have a device it will be removed, looked after by the trip leader and returned to the parent/carer. The child will be asked to unlock the device so that messages sent or received, any apps accessed or internet pages viewed whilst on the trip can be reviewed to assess any safeguarding risk. (refer to handling a nude or semi-nude image or selfie/upsurting incident). Parents/carers sign an agreement which acknowledge that Mobile devices are not allowed and will be searched if discovered.

Staff use of personal devices

- Staff will use a school phone where contact with students, parents or carers is required. In an emergency situation (such as a medical emergency whilst on a residential trip) staff may contact parents using a personal device with the agreement of the group leader.
- As part of recording children's learning journeys and experiences, staff may take pictures or recordings of pupils on a school device – personal devices must not be used. These must be saved onto the school system or, if intended to be shared via the school's social media, shared to the Assistant Head promptly. The images must then be deleted from the device and from any cloud based storage which they may have automatically uploaded to. Parents/carers give permission for photographs and videos to be shared via the 'use of digital images and video' form which is completed when children join the school.
- If a member of staff breaches the school policy about this, then disciplinary action may be taken.

Digital images and video

In this school:

- We gain parental/carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter/son joins the school (or annually).
- We do not identify pupils in online photographic materials.
- Staff sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones/personal equipment for taking pictures of pupils;
- The school blocks/filter access to social networking sites or newsgroups unless there is a specific approved educational purpose;
- Pupils are taught about how images can be manipulated in their online safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their ICT scheme of work;

- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location, such as house number, street name or school. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

Protecting Pupil Images Online

Burnt Ash Primary School recognises the increasing risks associated with the misuse of images online, including image manipulation using AI technologies.

In this school:

- We avoid unnecessarily identifying pupils
- We never link images to personal information
- Ensure only authorised staff publish content on the school's behalf
- We always consider whether images could make pupils easily identifiable
- Remove unnecessary location information or metadata before posting images
- Review images carefully before publication
- Where possible, images shared publicly will avoid close-up or front facing photographs that make children easily identifiable
- The school may use reduced resolution images for online publications where this supports safeguarding and reduces the risk of misuse

Burnt Ash Primary School regularly reviews its approach to image sharing to ensure it reflects emerging safeguarding risks.

Generative Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT, Google Gemini, Microsoft CoPilot and TeachMate AI.

Burnt Ash Primary School recognises that AI has many uses, including enhancing teaching and learning, and in helping to protect and safeguard pupils. However, AI may also have the potential to facilitate abuse (e.g. bullying, grooming & exploitation) and/or expose pupils to harmful content. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real.

Burnt Ash Primary School will treat any use of AI to access harmful content or bully pupils in line with this policy and our behaviour policy.

When using generative AI tools, staff must exercise caution and avoid processing any personal data through these platforms. It is essential to verify the accuracy of all AI-generated outputs before using them in any official capacity, as responsibility for correctness remains with staff members. Under no circumstances should pupil images, names, or any other identifying information be uploaded or shared with AI tools, ensuring compliance with data protection and safeguarding requirements

Remote Learning

Remote learning has become an essential component of education, offering flexibility and continuity during disruptions such as health crises, travel limitations, or emergencies. However,

increased online engagement also introduces risks like cyberbullying, phishing, and exposure to inappropriate content. To safeguard learners, our online safety policy emphasizes secure platforms, strong authentication, and clear guidelines for responsible digital behaviour, ensuring that remote learning remains both effective and safe.

To allow children safer access to the internet whilst approaching and completing their remote learning, At Burnt Ash:

- We use ILD (Reception and Y1&2) to share teaching videos and maintain communication with pupils via a secure platform in the event of a school, bubble closure or individual isolation.
- Links provided to websites and videos are assessed to ensure that pupils are accessing safe content.
- We share documents to support pupil's learning, including activities linked to teaching videos, with pupils by uploading them as part of an assignment.
- We use a range of Educational Websites to aid with children's learning within school and from home, these include: Mathletics, Purple Mash, Times Table Rockstars and Accelerated Reader. These websites will be used across the year groups to facilitate remote learning.
- Pupils are able to share their work with the whole class and access set assignments through Seesaw where they can like and comment on work from other pupils in their class. The work and comments uploaded are monitored and verified by a teacher before they are allowed on the class page.
- Teaching videos filmed by school staff are filmed either in a classroom or with a neutral background, ensuring that personal items are not on show.
- We provide a holistic, quality Online Safety education that provides children with the skills to recognise potential threats and respond to these using the appropriate strategies taught (SMART, BRECK). We provide this through weaving Online Safety teaching across the curriculum and within assemblies and explicit lessons using real life scenarios and stories applicable to the children's age group.

Updated: Autumn 2026

Next Review Date: Autumn 2027

Key Stage 1: Acceptable Use Agreement

I keep **SAFE online** because ...



I **CHECK** it's OK to use a website / game / app.

I **ASK** for help if I get lost online.

I **THINK** before I click on things.

I **KNOW** online people are really strangers.

I am **RESPONSIBLE** so never share private information.

I am **KIND** and polite online.

I **TELL** a trusted adult if I am worried about anything.

My trusted adults are:

My name:

--

Date signed _____

KS2 Pupil Online Acceptable Use Agreement

This agreement will help keep me safe and help me to be fair to others.

- ***I am an online digital learner*** – I use the school's IT for schoolwork, homework and other activities approved by trusted adults.
- ***I am a secure online learner*** - I keep my logins and passwords secret.
- ***I am careful online*** - I think before I click on links and only download when I know it is safe or has been agreed by trusted adults.
- ***I am guarded online*** - I only give out my full home address, phone number or other personal information that could be used to identify me or my family and friends when my trusted adults have agreed.
- ***I am cautious online*** - I know that some websites and social networks have age restrictions and I respect this and I only visit internet sites that I know my trusted adults have agreed.
- ***I am considerate online*** - I do not get involved with bullying or sharing inappropriate material.
- ***I am respectful online*** – I do not respond to unkind or hurtful messages/comments and tell my trusted adults if I receive these.
- ***I am responsible online*** – I keep others safe by talking to my trusted adults if a friend or person I know is being bullied or harassed online or is being affected by things they see or hear online. I speak with a trusted adult before I used AI tools.
- ***I am a creative digital learner online*** - I only edit or delete my own digital work and only use other people's work with their permission or where the work is shared through a Creative Commons licence.
- ***I am a researcher online*** - I use safer search tools approved by my trusted adults and know to 'double check' all information I find online.
- ***I communicate and collaborate online*** - with people I know and have met in real life or that a trusted adult has approved.
- ***I am SMART online*** - I understand that unless I have met people in real life, an online person is actually a stranger. I may sometimes want to meet these strangers so I will always ask my trusted adults for advice.

I have read and understood this agreement.

I know who are my trusted adults are and agree to the above.

Signed: _____

Date: _____

Acceptable Use Agreement: All Staff, Volunteers and Trustees

Covers use of all digital technologies in school: i.e. email, Internet, intranet, network resources, learning platform, software, communication tools, equipment and systems.



- I will only use the school's digital technology resources and systems for professional purposes or for uses deemed 'reasonable' by the Head teacher.

- I will not reveal my password(s) to anyone.
- I will not allow unauthorised individuals to access email/Internet/intranet/network, or other school systems.
- I will ensure all documents, data etc., are printed, saved, accessed and deleted / shredded in accordance with the school's network and data security protocols.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will only use the approved email system(s) for any school business. This is currently: Microsoft Outlook
- I will not browse, download or send material that is considered offensive or of an extremist nature by the school.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach or equipment failure to the online safety coordinator.
- I will not download any software or resources from the Internet that can compromise the network or might allow me to bypass the filtering and security system or are not adequately licensed.
- I will check copyright and not publish or distribute any work including images, music and videos, that is protected by copyright without seeking the author's permission.
- I will use Artificial Intelligence (AI) tools professionally and responsibly. I will not upload personal, confidential or sensitive information to AI systems. I will verify the accuracy of AI-generated content before using it in my professional practice.
- I understand that AI technologies can be used to create manipulated images, deepfakes and so-called 'nudification' images. Any concerns relating to image-based abuse, manipulated imagery or AI-generated content involving pupils will be treated as a safeguarding concern and reported immediately to the DSL.
- I will not connect any device (including USB flash drive), to the network that does not have up-to-date anti-virus software.
- I will not use personal digital cameras, mobile phones or personal devices to take, edit, store or transfer images or videos of pupils. Images must be taken with a school iPad and then transferred to the system before being deleted.
- I will only use school approved equipment for any storage, editing or transfer of digital images/videos and ensure I only save photographs and videos of children and staff on system (e.g. Teacher share)
- I understand that publicly shared images of pupils may be vulnerable to misuse or manipulation. I will not publish images on behalf of the school.
- AHT/Computing lead only: When publishing images on the school's social media, I will follow the school procedures relating to identifiability, images selection, metadata and safeguarding.
- I will ensure that my personal use of social media does not compromise my professional role, the reputation of the school, or the safety and wellbeing of pupils, families or colleagues.
- I will ensure, where used, I know how to use any social networking sites / tools securely, so as not to compromise my professional role.
- I understand that Burnt Ash Primary School is a mobile phone free working environment. Personal mobile phones must be stored securely and out of sight during the school day and may only be accessed during designated break periods in the staffroom and in offices away from children.

- I agree and accept that any computer or laptop loaned to me by the school, is provided solely to support my professional responsibilities.
- I will only access school resources remotely (such as from home) using Cisco and follow online safety protocols to interact with them.
- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I understand it is my duty to support a whole-school safeguarding approach and will report any behaviour of other staff or pupils, which I believe may be inappropriate or concerning in any way, to one of the DSLs.
- I understand that online safety is a safeguarding issue and that many safeguarding concerns may have an online element. I will consider online risks when responding to concerns about a child's welfare and will report concerns in line with school safeguarding procedures.
- I understand that all Internet and network traffic/usage can be logged and this information can be made available *to the Head/Safeguarding Lead* on their request.
- *Staff that have a teaching role only:* I will embed the school's on-line safety/digital literacy / counter extremism curriculum into my teaching.

User Signature

I agree to abide by all the points above.

I understand that I have a responsibility for my own and others online safeguarding and I undertake to be a 'safe and responsible digital technologies user'.

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent online safety policies.

I understand that failure to comply with this agreement could lead to disciplinary action.

Signature Date

Full Name (printed)

Job title / Role



Online Safety agreement form: parents

Internet and ICT:

- As the parent or legal guardian of the pupil(s) named below, I grant permission for the school to give my *daughter/son* access to:

- the Internet at school
 - ICT facilities and equipment at the school.
 - Educational online software, including mathletics, frog play, purple mash & Seesaw.
- I understand that the school uses filtering systems but that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies. I understand that the school takes every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials.
 - I understand that the school can, if necessary, check my child's computer files, the Internet sites they visit at school and monitor how apps and programs are used. If there are concerns about my child's online safety or e-behaviour they will contact me.

Use of digital images, photography and video:

- I understand the school has a clear policy on "The use of digital images and video" and I agree to all of the points stated in this.
- I understand that the school will use photographs/video material to support learning activities where necessary.
- I accept that the school may use photographs/video that includes my child in publicity that reasonably promotes the work of the school, and for no other purpose.
- I will not take and then share online, photographs of other children at school events without permission.

Social networking and media sites:

- I understand that the school has a clear policy on "The use of social networking and media sites" and I support this.
- I understand that the school takes any inappropriate behaviour seriously and will respond to observed or reported inappropriate or unsafe behaviour.
- I understand that my son/daughter has agreed in the pupil acceptable-use policy not to search for or share any material that could be considered offensive, harmful or illegal. This might include bullying or extremist/hate/discriminatory content.
- I will support the school by promoting safe use of the Internet and digital technology, including AI tools, at home and regularly monitor my child's online activity and profile, particularly regarding their use of social media. I will inform the school if I have any concerns.

My daughter/son name(s): _____

Parent / guardian signature: _____

Date: ____/____/____



The use of digital images and video

To comply with UK data protection legislation, we require your permission before taking photographs or making video recordings of your child.

Images and Video Used Within School

As part of celebrating children's work and achievements, we may take photographs or video recordings of pupils using school owned devices. These images may include clear, identifiable photographs of individual pupils and small groups.

These images will be used for internal purposes only, including:

- classroom displays
- learning journals and exercise books
- assemblies and celebrations
- displays around the school
- internal presentations and staff training
- Photographs shared directly with the parents/carers only, for example, through ILD

All images and videos will be captured and stored securely using school systems.

Images and Video Used Online or in Public-Facing Publications

Where images or videos are intended for publication on the school website, social media pages, newsletters, or other promotional materials, we take additional steps to protect pupils' privacy.

This includes:

- using photographs taken from a distance rather than close-up portraits
- using group images rather than individual pupil photographs
- avoiding images where pupils are the sole focus of the photograph
- selecting images that do not prominently show pupils' faces
- reducing image resolution where appropriate
- removing embedded metadata and location information before publication
- carefully reviewing images prior to publication to minimise the risk of identification.

Media Coverage

On rare occasions, photographers or film crews from external media organisations may attend school events. Where appropriate, we will take reasonable steps to ensure that pupils are represented safely and respectfully and will follow any consent preferences recorded by parents and carers.



The use of social networking and on-line media

This school asks its whole community to promote the 3 commons approach to online behaviour:

- Common courtesy

- Common decency
- Common sense

How do we show common courtesy online?

- We ask someone's permission before uploading photographs, videos or any other information about them online.
- We do not write or upload 'off-hand', hurtful, rude or derogatory comments and materials. To do so is disrespectful and may upset, distress, bully or harass.

How do we show common decency online?

- We do not post comments that can be considered as being **intimidating, racist, sexist, homophobic or defamatory. This is online bullying** and may be harassment or libel.
- When such comments exist online, we do not forward such emails, tweets, videos, etc. By creating or forwarding such materials we are all liable under the law.

How do we show common sense online?

- We think before we click.
- We think before we upload comments, photographs and videos.
- We think before we download or forward any materials.
- We think carefully about what information we share with others online, and we check where it is saved and check our privacy settings.
- We make sure we understand changes in use of any web sites we use.
- We block harassing communications and report any abuse.

Any actions online that impact on the school and can potentially lower the school's (or someone in the school) reputation in some way or are deemed as being inappropriate will be responded to.

In the event that any member of staff, student or parent/carer is found to be posting libellous or inflammatory comments on Facebook or other social network sites, they will be reported to the appropriate 'report abuse' section of the network site.

(All social network sites have clear rules about the content which can be posted on the site and they provide robust mechanisms to report contact or activity which breaches this.)

In serious cases we will also consider legal options to deal with any such misuse.

The whole school community is reminded of the CEOP process for reporting inappropriate sexual approaches towards children at: <https://www.thinkuknow.co.uk/parents/>