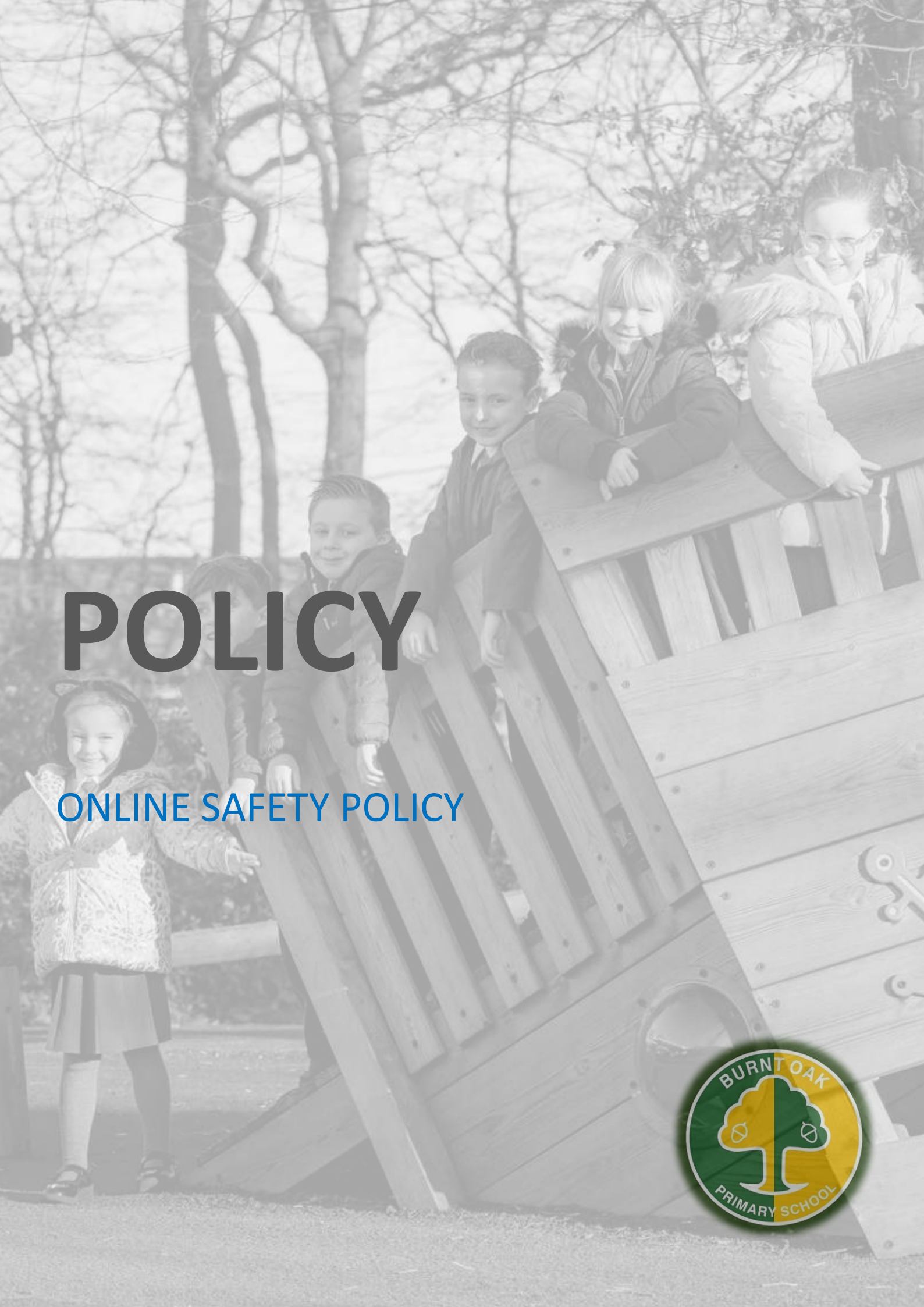

POLICY

ONLINE SAFETY POLICY

"We all flourish from a wealth of learning experiences that positively impact on our academic, physical and emotional success"

POLICY DETAILS

Policy Title:	**Online Safety Policy**
Version:	1.0
Date created:	Autumn 2025
Purpose:	To set out how the school keeps children, staff, and the wider community safe when using digital technologies. Its purpose is both protective and educational.
Approved by EHT:	Autumn 2025
Next Review:	Autumn 2026

POLICY HISTORY

Version:	Date:	Changes:
1.0	Autumn 25	New policy format

CONTENTS

1. AIMS

The purpose of the Burnt Oak Primary School Online Safety Policy is to:

- Safeguard and protect all members of Burnt Oak Primary School community online
- Identify approaches to educate and raise awareness of online safety throughout the community
- Enable all staff to work safely and responsibly, to role model positive behaviour online and to manage professional standards and practice when using technology
- Identify clear procedures to use when responding to online safety concerns
- Ensure online safety is embedded within our whole-school safeguarding approach

This policy should be read in conjunction with our:

- Child Protection and Safeguarding Policy
- Behaviour Policy
- Anti-Bullying Policy
- Mobile Phone Policy
- Acceptable Use Policies (for staff, pupils, and visitors)
- Data Protection Policy
- RSHE Policy

2. ROLES & RESPONSIBILITIES

2.1 GOVERNING BODY

- The governing body has overall responsibility for ensuring the school meets its statutory duties regarding online safety
- The governing body will review this policy annually

2.2 DESIGNATED SAFEGUARDING LEAD (DSL)

- The DSL has overall responsibility for safeguarding, including online safety
- All online safety incidents with safeguarding implications must be reported to the DSL immediately
- The DSL will ensure that online safety training is included in all safeguarding training

2.3 ONLINE SAFETY LEAD

- The school has appointed Laura King (Computing Leader) to be the Online Safety Lead
- The Online Safety Lead works closely with the Designated Safeguarding Lead (DSL) to ensure online safety is integrated into our safeguarding framework

2.4 ALL STAFF

- Burnt Oak Primary School recognises that all members of the community have important roles and responsibilities to play with regards to online safety
- All staff have a responsibility to provide a safe environment in which children can learn

- All staff are made aware of systems within their school which support safeguarding, and these are explained to them as part of staff induction

3. LEGAL FRAMEWORK AND STATUTORY DUTIES

This policy is based on the following legislation and guidance:

- Keeping Children Safe in Education (KCSIE) 2025 - statutory guidance
- Working Together to Safeguard Children - statutory guidance
- Relationships, Sex and Health Education (RSHE) statutory guidance (from September 2026)
- Education Act 2011 - powers to search and confiscate
- Computer Misuse Act 1990
- Data Protection Act 2018 and UK GDPR
- Equality Act 2010
- The Education and Inspections Act 2006 - powers to regulate conduct of pupils

4. WHOLE-SCHOOL APPROACH TO ONLINE SAFETY

Online safety should be set in the context of a wider whole-school approach to supporting pupils to be safe, happy and prepared for life beyond school. The curriculum on online safety should complement, and be supported by, the school's wider policies on behaviour, inclusion, respect for equality and diversity, bullying and safeguarding Relationships Education, Relationships and Sex Education and Health Education.

Online safety is embedded across our curriculum and is part of our safeguarding culture. We recognise that:

- Safeguarding and promoting the welfare of children is everyone's responsibility
- School and college staff are particularly important, as they are in a position to identify concerns early, provide help for children, promote children's welfare and prevent concerns from escalating
- Technology is an integral part of children's lives both in and out of school

5. TEACHING AND LEARNING

5.1 WHY INTERNET USE BENEFITS EDUCATION

- Internet use is part of the statutory curriculum and is a necessary tool for learning
- The school has a duty to provide pupils with quality Internet access as part of their learning experience
- Pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security
- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions
- Internet access is an entitlement for pupils who show a responsible and mature approach to its use

5.2 BENEFITS OF USING THE INTERNET IN EDUCATION INCLUDE

- Access to worldwide educational resources including museums and art galleries

- Educational and cultural exchanges between pupils worldwide
- Vocational, social and leisure use in libraries, clubs and at home
- Access to experts in many fields for pupils and staff
- Professional development for staff through access to national developments, educational materials and effective curriculum practice
- Professional development for staff via National College
- Collaboration across networks of schools, support services and professional associations
- Improved access to technical support including remote management of networks and automatic system updates
- Exchange of curriculum and administration data with Medway Council and the DfE
- Access to learning wherever and whenever convenient through the use of Chromebooks and Google tools for education
- Targeted support when physical school access is restricted
- Pupils gain skills in using real-life tools such as Google docs, slides, forms etc.
- Each class has a virtual Google classroom for sharing lesson resources and evidencing learning. This is not limited to resources for in the classroom and will provide parents and pupils access to supporting resources at home

5.3 HOW INTERNET USE ENHANCES LEARNING

- Pupils will be taught about acceptable use of the Internet and will be given clear objectives for Internet use
- Access levels to the internet will be reviewed to reflect the curriculum requirements and the age and ability of pupils
- Staff should guide pupils to online activities that will support the learning outcomes planned for the pupils' age and ability
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work

5.4 ONLINE SAFETY EDUCATION

- Online safety is embedded across the curriculum and taught explicitly to all pupils through the use of Purple Mash
- Internet Safety Day (February) is used to stimulate meaningful discussions about online safety both in assembly and the classroom
- All staff receive appropriate safeguarding and child protection training (including online safety which, amongst other things, includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring) at induction. The training is regularly updated. In addition, all staff receive

safeguarding and child protection (including online safety) updates (for example, via email, e-bulletins, and staff meetings), as required, and at least annually

- Pupils will be taught to recognise and respond to online safety risks including:
    - Misinformation, disinformation (including fake news), and conspiracy theories
    - Online sexual abuse and exploitation
    - Child-on-child abuse (including sexual violence and harassment)
    - Cyberbullying
    - Radicalisation and extremism (Prevent duty)
    - Sharing of personal information and images
    - Inappropriate content
    - Online grooming
    - Commercial exploitation

6. EVALUATING INTERNET CONTENT

- Pupils will use age-appropriate tools to research Internet content
- The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum
- In KS2, as part of the Computing Curriculum, pupils will use search technologies effectively, appreciate how results are selected and ranked, and be discerning in evaluating digital content

7. RELATIONSHIPS, SEX AND HEALTH EDUCATION (RSHE)

RSHE should be sensitive to the religious background of pupils, and schools must ensure they comply with the relevant provisions of the Equality Act 2010, under which religion or belief are amongst the protected characteristics Relationships and Sex Education Statutory Guidance.

Our online safety education complements our RSHE curriculum by teaching pupils about:

- Healthy and respectful online relationships
- The risks of sharing personal information and images online
- How to recognise and report inappropriate online contact
- Understanding consent in an online context
- Respectful online communication

Schools should avoid language and activities which repeat or enforce gender stereotypes. Schools should be mindful to avoid any suggestion that social transition is a simple solution to feelings of distress or discomfort

When teaching about online safety in relation to relationships, we will:

- Support young people to develop the skills they need to build healthy relationships. Pupils should understand that anyone can be a victim of sexual violence, regardless of sex, sexual orientation, gender reassignment or any other protected characteristic, and that the victim is never to blame Relationships and Sex Education Statutory Guidance
- Ensure pupils understand how to report concerns both within school and to external services
- Ensure that all staff know what to do if they have concerns that a pupil is being neglected or abused. Pupils should understand how confidentiality will be handled in a lesson and what might happen if they choose to make a report, about themselves or a peer. Pupils should also understand where they can report any concerns and seek help, including to external services if they do not feel comfortable talking to school staff

8. VULNERABLE PUPILS

Children with special educational needs or disabilities (SEND) or certain medical or physical health conditions can face additional safeguarding challenges both online and offline

Burnt Oak Primary School is aware that some pupils are considered to be more vulnerable online due to a range of factors. This may include, but is not limited to:

- Children in care
- Children with Special Educational Needs and Disabilities (SEND) or mental health needs
- Children with English as an additional language (EAL)
- Children experiencing trauma or loss

Additional barriers can exist when recognising abuse, neglect and exploitation in this group of children. These can include:

- Assumptions that indicators of possible abuse such as behaviour, mood and injury relate to the child's condition without further exploration
- These children being more prone to peer group isolation or bullying (including prejudice-based bullying) than other children
- The potential for children with SEND or certain medical conditions being disproportionately impacted by behaviours such as bullying, without outwardly showing any signs
- Communication barriers and difficulties in managing or reporting these challenges
- Cognitive understanding - being unable to understand the difference between fact and fiction in online content and then repeating the content/behaviours in schools or colleges or the consequences of doing so

Our approach:

- Differentiated and ability-appropriate online safety education, access and support is provided to vulnerable pupils

- When needed we will seek input from specialist staff as appropriate, including the SENCO
- Any reports of abuse involving children with SEND will require close liaison with the designated safeguarding lead (or a deputy) and the special educational needs coordinator (SENCO) Keeping Children Safe in Education Keeping Children Safe in Education
- We will consider extra pastoral support and attention for these children, along with ensuring any appropriate support for communication is in place

9. MANAGING INFORMATION SYSTEMS

9.1 INFORMATION SYSTEMS SECURITY

- Virus protection will be updated regularly
- Personal data sent over the Internet or taken off site will be encrypted
- Unapproved software will not be allowed in work areas or attached to emails
- Files held on the school's network will be regularly checked
- The IT technician will review system capacity regularly
- The use of user logins and passwords to access the school network will be enforced
- Where data is uploaded to a cloud-based platform, this is part of the EU Safe Harbour

9.2 EMAIL MANAGEMENT

- Pupils may only use approved school email accounts for school purposes
- Pupils must immediately tell a designated member of staff if they receive offensive email
- Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult
- Whole-class or group email addresses will be used for communication outside of the school
- Staff will only use official school-provided email accounts to communicate with pupils and parents/carers, as approved by the Senior Leadership Team
- Access in school to external personal email accounts may be blocked
- Excessive social email use can interfere with learning and will be restricted
- Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper would be
- The forwarding of chain messages is not permitted
- Staff should not use personal email accounts during school hours or for professional purposes

9.3 PUBLISHED CONTENT MANAGEMENT

- The contact details on the website should be the school address, email and telephone number. Staff or pupils' personal information must not be published
- Email addresses will be published carefully online, to avoid being harvested for spam (e.g. by replacing '@' with 'AT')

- The Headteacher will take overall editorial responsibility for online content published by the school and will ensure that content published is accurate and appropriate
- The school website will comply with the school's guidelines for publications including respect for intellectual property rights, privacy policies and copyright

9.4 PUBLISHING PUPILS' IMAGES OR WORK

- Images or videos that include pupils will be selected carefully and will not provide material that could be reused
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs
- Written permission from parents or carers will be obtained before images/videos of pupils are electronically published
- Pupils' work will only be published with permission from parents or carers
- Written consent will be kept by the school where pupils' images are used for publicity purposes, until the image is no longer in use

9.5 SOCIAL NETWORKING, SOCIAL MEDIA AND PERSONAL PUBLISHING

- The school will control access to social media and social networking sites
- Pupils will be advised never to give out personal details of any kind which may identify them and/or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests/clubs etc.
- Staff official blogs or wikis should be password protected and run from the school website with approval from the Senior Leadership Team. Members of staff are advised not to run social network spaces for pupil use on a personal basis
- Personal publishing will be taught via age-appropriate sites that are suitable for educational purposes. They will be moderated by the school where possible
- Pupils will be advised on security and privacy online and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications
- Pupils will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private
- All members of the school community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory
- All members of the school community should have the permission of staff before publishing photographic images of them
- Newsgroups will be blocked unless a specific use is approved
- Concerns regarding pupils' use of social networking, social media and personal publishing sites (in or out of school) will be raised with their parents/carers, particularly when concerning pupils' underage use of sites

- Through curriculum lessons, pupils will be made aware of the risks of social media sites (Instagram, Facebook, TikTok, Snapchat etc.) as well as the dangers involved in cyberbullying, youth produced sexual imagery (sexting), and online gaming
- Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and safe and professional behaviour will be outlined in the school Acceptable Use Policy
- Where students attempt to make contact with staff members through private social media channels, such requests should be denied by the staff member, logged in the online safety log, the child spoken to and parent/carer informed by the class teacher
- All staff are aware of systems within school which support safeguarding, and these are explained to them as part of staff induction.

10. FILTERING AND MONITORING

All staff receive appropriate safeguarding and child protection training (including online safety which, amongst other things, includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring)

10.1 FILTERING

- The school's broadband access will include filtering appropriate to the age and maturity of pupils
- The school will work with Medway Council to ensure that filtering policy is continually reviewed
- The school will have a clear procedure for reporting breaches of filtering. All members of the school community (all staff and all pupils) will be aware of this procedure
- If staff or pupils discover unsuitable sites, the URL will be reported to the School Online Safety Coordinator who will then record the incident and escalate
- The School filtering system will block all sites on the Internet Watch Foundation (IWF) list.
- Changes to the school filtering policy will be risk assessed by staff with educational and technical experience prior to any changes and where appropriate with consent from the Senior Leadership Team.
- The School Senior Leadership Team will ensure that regular checks are made to ensure that the filtering methods selected are effective.
- Any material that the school believes is illegal will be reported to appropriate agencies such as IWF, Medway Police or CEOP.
- The school's access strategy will be designed by educators to suit the age and curriculum requirements of the pupils, with advice from network managers.
- The school will have regard to the DfE's guidance on generative AI: product safety expectations to ensure safe use of AI tools and understand filtering and monitoring requirements around AI. The school will use the DfE's 'plan technology for your school' service to self-assess against filtering and monitoring standards and receive personalised recommendations.

10.2 HOW WILL VIDEOCONFERENCING BE MANAGED?

- Equipment connected to the educational broadband network should use the national E.164 numbering system and display their H.323 ID name.
- External IP addresses will not be made available to other sites.
- Videoconferencing contact information will not be put on the school Website.
- The equipment must be secure and if necessary locked away when not in use.
- School videoconferencing equipment will not be taken off school premises without permission.
- Responsibility for the use of the videoconferencing equipment outside school time will be established with care.
- Teacher/pupil contact will only be made through specially designated school email addresses and with prior informed consent from parents/carers.

11. USERS

- Parents and carers permission should be obtained prior to children taking part in videoconferences.
- Only key administrators should be given access to videoconferencing administration areas or remote control pages.
- Unique log on and password details for the educational videoconferencing services should only be issued to members of staff and kept secure.

12. HOW ARE EMERGING TECHNOLOGIES MANAGED

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Pupils will be instructed about safe and appropriate use of personal devices both on and off site in accordance with the school Acceptable Use and Mobile Phone Policy.

13. POLICY DECISIONS

13.1 HOW WILL INTERNET ACCESS BE AUTHORISED?

- Parents will be asked to read the School Acceptable Use Policy for pupil access and discuss it with their child, where appropriate.
- All visitors to the school site who require access to the school's network or internet access will be asked to read and sign an Acceptable Use Policy.
- Parents / carers will be informed that pupils will be provided with supervised Internet access appropriate to their age and ability.
- When considering access for vulnerable members of the school community (such as with children with special education needs) the school will make decisions based on the specific needs and understanding of the pupil(s).
- At Key Stage 1 pupils' access to the Internet will be by adult demonstration with occasional directly supervised access to specific and approved online materials such as TTRS, Purple Mash and EdShed.

- At Key Stage 2 pupils will be supervised. Pupils will use age-appropriate search engines, online tools and online activities will be teacher-directed where necessary.

13.2 HOW WILL RISKS BE ASSESSED?

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor Medway council can accept liability for the material accessed, or any consequences resulting from Internet use.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to Kent Police.
- Methods to identify, assess and minimise risks will be reviewed regularly.

13.3 HOW WILL THE SCHOOL RESPOND TO ANY INCIDENTS OF CONCERN?

- All members of the school community will be informed about the procedure for reporting e-Safety concerns (such as breaches of filtering, cyberbullying, Sexting, illegal content etc.).
- The e-Safety Coordinator will record all reported incidents and actions taken in the School e-Safety incident log and other in any relevant areas e.g. Behaviour or safeguarding log.
- The Designated Safeguarding Lead will be informed of any e-Safety incidents involving safeguarding concerns, which will then be escalated appropriately.
- The school will manage e-Safety incidents in accordance with the school behaviour policy where appropriate.
- The school will inform parents/carers of any incidents of concerns as and when required.
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes required.
- Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact the Children's Safeguarding Team or e-Safety Officer and escalate the concern to the Police (this includes: cyber-bullying resulting in emotional abuse).
- If the school is unsure how to proceed with any incidents of concern, then the incident will be escalated to the Children's Safeguarding Team or Local Authority (Medway Council).
- If an incident of concern needs to be passed beyond the school then the concern will be escalated to the e-Safety Officer to communicate to other schools in Medway.

14. PROCEDURES FOR RESPONDING TO SPECIFIC ONLINE INCIDENTS OR CONCERNS

14.1 YOUTH PRODUCED SEXUAL IMAGERY OR "SEXTING"

- Burnt Oak Primary recognises youth produced sexual imagery (known as "sexting") as a safeguarding issue; therefore all concerns will be reported to and dealt with by the Designated Safeguarding Lead.

- The school will follow the advice as set out in the non-statutory UKCCIS guidance: 'Sexting in schools and colleges: responding to incidents and safeguarding young people' and MSCB guidance: 'Sexting' in schools: advice and support around self-generated images'.
- The school will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery.

14.2 ONLINE CHILD SEXUAL ABUSE AND EXPLOITATION

- We will ensure that all members of the community are aware of online child sexual abuse, including: exploitation and grooming; the consequences; possible approaches which may be employed by offenders to target children and how to respond to concerns.
- Burnt Oak recognises online child sexual abuse as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the Designated Safeguarding Lead.

14.3 CYBERBULLYING

- Cyberbullying, along with all other forms of bullying, will not be tolerated at Burnt Oak Primary School.
- Full details of how the school will respond to cyberbullying are set out in the Anti-bullying policy.

14.4 VIRAL HOAXES OR SOCIAL MEDIA 'CHALLENGES'

Incidents concerning social media 'challenges' or viral hoaxes should be dealt with in accordance with advice from the UK Safer Internet Centre. In short staff will:

- Remain calm and research the phenomenon carefully (be critical of news articles as these are often sensationalised and inaccurate).
- Avoid showing or naming specific content as this may fuel curiosity.
- Remind children to report and block inappropriate or upsetting content.
- Engage with parents/carers appropriately, avoid fuelling panic by naming or showing specific phenomena. Remind parents of the importance of basic internet safety principles.

14.5 HOW WILL E-SAFETY COMPLAINTS BE HANDLED?

- Complaints about Internet misuse will be dealt with under the School's Complaints Policy.
- Any complaint about staff misuse will be referred to the Headteacher.
- All e-Safety complaints and incidents will be recorded by the school, including any actions taken.
- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils will need to work in partnership with the school to resolve issues.
- All members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns.
- Discussions will be held with the Police and/or Children's Safeguarding Team to establish procedures for handling potentially illegal issues.

- Any issues (including sanctions) will be dealt with according to the school's behaviour and safeguarding procedures.
- All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community.

14.6 HOW IS THE INTERNET USED ACROSS THE COMMUNITY?

- The school will liaise with local organisations to establish a common approach to e-Safety.
- The school will be sensitive to Internet-related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.
- The school will provide appropriate levels of supervision for pupils who use the internet and technology whilst on the school site.
- The school will provide an AUP for any guest who needs to access the school computer system or internet on site.

14.7 HOW WILL CYBERBULLYING BE MANAGED?

- Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's policies on anti-bullying and behaviour.
- All incidents of cyberbullying reported to the school will be recorded.
- There will be clear procedures in place to investigate incidents or allegations of Cyberbullying.
- Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.
- The school will take steps to identify the bully, where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- Pupils, staff and parents/carers will be required to work with the school to support the approach to cyberbullying and the school's e-Safety ethos.
- Sanctions for those involved in cyberbullying may include:
    - The bully will be asked to remove any material deemed to be inappropriate or a service provider may be contacted to remove content if the bully refuses or is unable to delete content.
    - Internet access may be suspended at school for the user for a period of time. Other sanctions for pupils and staff may also be used in accordance to the schools anti-bullying, behaviour policy or Acceptable Use Policy.
    - Parent/carers of pupils will be informed.
    - The Police will be contacted if a criminal offence is suspected.

14.8 HOW WILL LEARNING PLATFORMS BE MANAGED?

- The senior leadership team (SLT) and staff will regularly monitor the usage of the LP by pupils and staff in all areas, in particular message and communication tools and publishing facilities.
- Pupils/staff will be advised about acceptable conduct and use when using the LP.
- Only members of the current pupil, parent/carers and staff community will have access to the LP.
- All users will be mindful of copyright issues and will only upload appropriate content onto the LP.
- When staff, pupils etc. leave the school their account or rights to specific school areas will be disabled or transferred to their new establishment.
- Any concerns about content on the LP may be recorded and dealt with in the following ways:
    - The user will be asked to remove any material deemed to be inappropriate or offensive.
    - The material will be removed by the site administrator if the user does not comply.
    - Access to the LP for the user may be suspended.
    - The user will need to discuss the issues with a member of SLT before reinstatement.
    - A pupil's parent/carer may be informed.
- A visitor may be invited onto the LP by a member of the SLT. In this instance there may be an agreed focus or a limited time slot.
- Pupils may require editorial approval from a member of staff. This may be given to the pupil to fulfil a specific aim and may have a limited time frame.

14.9 HOW WILL MOBILE PHONES AND PERSONAL DEVICES BE MANAGED?

- The use of mobile phones and other personal devices by pupils and staff in school will be decided by the school and is covered in the school Acceptable Use and Mobile Phone Policies.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the school community and any breaches will be dealt with as part of the school's behaviour policy and logged in the e-Safety log book.
- School staff may confiscate a phone or device if they believe it is being used to contravene the schools behaviour or anti-bullying policy. The phone or device might be searched by the Senior Leadership team with the consent of the pupil or parent/carer. If there is suspicion that the material on the mobile may provide evidence relating to a criminal offence the phone will be handed over to the police for further investigation.
- Mobile phones and personal devices will not be used during lessons or formal school time. They should be switched off at all times.
- The Bluetooth function of a mobile phone should be switched off at all times and not be used to send images or files to other mobile phones.
- Electronic devices of all kinds that are brought in to school are the responsibility of the user. The school accepts no responsibility for the loss, theft or damage of such items. Nor will the school accept responsibility for any adverse health effects caused by any such devices, either potential or actual.

- Mobile phones and personal devices are not permitted to be used in certain areas within the school site such as changing rooms and toilets.

15. PUPILS USE OF PERSONAL DEVICES

- If a pupil breaches the school policy 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/carers in accordance with the school policy.
- Phones and devices must not be taken into examinations. Pupils found in possession of a mobile phone during an exam will be reported to the appropriate examining body. This may result in the pupil's withdrawal from either that examination or all examinations.
- If a pupil needs to contact his/her parents/carers they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.
- Pupils should protect their phone numbers by only giving them to trusted friends and family members. Pupils will be instructed in safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences.

16. STAFF USE OF PERSONAL DEVICES

(Please refer to the Mobile Phone Policy)

- Staff will only be permitted to use their mobile phones to access school emails where the device can be locked using a password (use of a swipe code is not acceptable). Staff should protect the security of their mobile phone by never sharing their password, regularly changing their password and locking the device when not in use. Staff must also know how to remotely wipe their device to factory defaults if it is lost or stolen.
- Staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity, except in exceptional circumstances (e.g. during self-isolation) and only when approved by a member of the Senior Leadership Team. In these circumstances, staff must withhold their telephone number.
- Staff will be issued with a school phone where contact with pupils or parents/carers is required.
- Mobile Phone and devices will be switched off or switched to 'silent' mode, Bluetooth communication should be "hidden" or switched off and mobile phones or devices will not be used during teaching periods unless permission has been given by a member of the Senior Leadership Team in emergency circumstances.
- If members of staff have an educational reason to allow children to use mobile phones or personal device as part of an educational activity then it will only take place when approved by the Senior Leadership Team.
- Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use work-provided equipment for this purpose.
- If a member of staff breaches the school policy then disciplinary action may be taken.

17. COMMUNICATION POLICY

17.1 HOW WILL THE POLICY BE INTRODUCED TO PUPILS?

- All users will be informed that network and Internet use will be monitored.
- Pupil instruction regarding responsible and safe use will precede Internet access.
- e-Safety (digital literacy) will be taught during computing lessons at the beginning of each term; covering both safe school and home use.
- Teachers will deliver e-safety lessons from the Purple Mash scheme of work.
- e-Safety training will be part of the transition programme across the Key Stages and when moving between establishments.
- e-Safety rules or copies of the student Acceptable Use Policy will be posted in all rooms with Internet access.
- Safe and responsible use of the Internet and technology will be reinforced across the curriculum and subject areas.
- Particular attention to e-Safety education will be given where pupils are considered to be vulnerable.
- All pupils will be taught how to report an incident.

17.2 HOW WILL THE POLICY BE DISCUSSED WITH STAFF?

- The e-Safety Policy will be formally provided to and discussed with all members of staff.
- Training will be provided annually by the Computing Leader via National College.
- To protect all staff and pupils, the school will implement Acceptable Use Policies.
- Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff.
- Staff who manage filtering systems or monitor ICT use will be supervised by the Senior Leadership Team and have clear procedures for reporting issues.
- The School will highlight useful online tools which staff should use with children in the classroom. These tools will vary according to the age and ability of the pupils.
- All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

17.3 HOW WILL PARENTS' SUPPORT BE ENLISTED?

- Parents/carers' attention will be drawn to the school e–Safety Policy in newsletters and on the school website.
- Parents/carers will be informed of online safety rules and expectations regarding educational sites, social networks and email via a parent's information letters.

- A partnership approach to e-Safety at home and at school with parents will be encouraged. This may include offering parent evenings with demonstrations and suggestions for safe home Internet use, or highlighting e-Safety at other attended events e.g. parent evenings and sports days.
- Parents will be requested to sign an e-Safety/Internet agreement as part of the Home School Agreement.
- Parents will be encouraged to read the school Acceptable Use Policy for pupils and discuss it's implications with their children.
- Information and guidance for parents on e–Safety will be made available to parents in a variety of formats.
- Advice on useful resources and websites, filtering systems and educational and leisure activities which include responsible use of the Internet will be made available to parents.
- Interested parents will be referred to organisations listed in the "e-Safety Contacts and References section".
- Where concerns are raised in school about particular apps or trends, blanket communications will be sent to all parents/carers with advice and age-ratings through SchoolsBuddy.
- Parents will be encouraged to complete a parent online safety webinar on National College
- Weekly posts on social media will share that week's 'wake up Wednesday' from National College.

17.4 HOW WILL PERSONAL DATA BE PROTECTED?

Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulation (GDPR) and The Data Protection Act 2018 and the Freedom of Information Act.