Policy Title	**ONLINE SAFETY POLICY**
Committee responsible	Ethos & Curriculum committee
Last reviewed	November 2023
Next review due	November 2026
Who is governed by this policy	Staff, governors, pupils, parents
Available on website	**YES**

ONLINE SAFETY POLICY

1. Introduction

This Online Safety Policy outlines the commitment of Warnham CE Primary School to safeguard members of our school community online in accordance with statutory guidance and best practice.

The policy applies to all members of the school community (including staff, pupils, governors, volunteers, parents and carers, visitors, community users) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site.

Warnham CE Primary School will deal with such incidents and associated behaviour within this policy and our anti-bullying policy and will, where known, inform parents / carers of incidents of inappropriate online safety behaviour that take place out of school.

2. Scope

This Online Safety Policy:

- sets expectations for the safe and responsible use of digital technologies for learning, administration, and communication
- is regularly reviewed, taking account of online safety incidents and changes / trends in technology and related behaviours
- establishes guidance for staff in how they should use digital technologies responsibly, protecting themselves and the school and how they should use this understanding to help safeguard learners in the digital world
- describes how the school will help prepare pupils to be safe and responsible users of online technologies
- establishes clear procedures to identify, report, respond to and record the misuse of digital technologies and online safety incidents, including external support mechanisms
- is supplemented by a series of related Acceptable Use Policies
- is made available to staff at induction
- is published on the school website.

3. Responsibilities

To ensure the online safeguarding of members of our school community it is important that all members of that community work together to develop safe and responsible online behaviours, learning from each other and from good practice elsewhere, reporting inappropriate online behaviours, concerns, and misuse as soon as these become apparent. While this will be a team effort, the following outlines the online safety roles and responsibilities of individuals and groups within the school.

Headteacher and Senior Leaders

The headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding as the Designated Safeguarding Lead, as defined in Keeping Children Safe in Education.

The headteacher and at least one other member of the senior leadership team is aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.

The headteacher / senior leaders are responsible for ensuring that the Designated Safeguarding Lead / IT provider and other relevant staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and train other colleagues, as relevant.

The headteacher / senior leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role.

The headteacher / senior leaders will work with the responsible Governor and IT service providers in all aspects of filtering and monitoring.

Governors

The DfE guidance "Keeping Children Safe in Education" states:
"Governing bodies and proprietors should ensure there are appropriate policies and procedures in place in order for appropriate action to be taken in a timely manner to safeguard and promote children's welfare …. this includes … online safety"

"Governing bodies and proprietors should ensure an appropriate senior member of staff, from the school or college leadership team, is appointed to the role of designated safeguarding lead. The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place)"

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

A member of the governing body will take on the role of Online Safety Governor to include:

- regular meetings with the Designated Safeguarding Lead
- regularly receiving (collated and anonymised) reports of online safety incidents
- checking that provision outlined in the Online Safety Policy (e.g. online safety education provision and staff training is taking place as intended)
- ensuring that the filtering and monitoring provision is reviewed and recorded, at least annually
- reporting to the Full Governing Body

The governing body will also support the school in encouraging parents / carers and the wider community to become engaged in online safety activities.

Designated Safeguarding Lead (DSL)

Keeping Children Safe in Education states that:
"The designated safeguarding lead (DSL) should take lead responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place). This should be explicit in the role holder's job description.".

The DSL "is able to understand the unique risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online at school or college"

The DSL "can recognise the additional risks that children with special educational needs and disabilities (SEND) face online, for example, from bullying, grooming and radicalisation and are confident they have the capability to support children with SEND to stay safe online".

The DSL will:

- hold the lead responsibility for online safety, within their safeguarding role

- meet regularly with the online safety governor to discuss current issues, review (anonymised) incidents and filtering and monitoring logs and ensuring that annual (at least) filtering and monitoring checks are carried out
- attend relevant governing body meetings
- be responsible for receiving reports of online safety incidents and deciding whether to make a referral by liaising with relevant agencies, ensuring that all incidents are recorded
- liaise with staff and IT providers on matters of safety and safeguarding and welfare (including online and digital safety)

Curriculum Leads

Curriculum Leads will work with the DSL to develop a planned and coordinated online safety education programme e.g. ProjectEVOLVE .

This will be provided through:

- PHSE and SRE programmes
- assemblies and pastoral programmes
- through relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week
- computing lessons

Teaching & Support Staff

School staff are responsible for ensuring that:

- they have an awareness of current online safety matters / trends and of the current Online Safety Policy and practices
- they understand that online safety is a core part of safeguarding
- they have read, understood, and signed the staff Acceptable Use Policy (AUP)
- they immediately report any suspected misuse or problem to the DSL for investigation / action, in line with the school safeguarding procedures
- all digital communications with learners and parents / carers are on a professional level and only carried out using official school systems
- online safety issues are embedded in all aspects of the curriculum and other activities
- ensure learners understand and follow the Online Safety Policy and Acceptable Use Policies
- they supervise and monitor the use of digital technologies, mobile devices, cameras, etc., in lessons and other school activities (where allowed) and implement current policies regarding these devices
- in lessons where internet use is pre-planned, learners are guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- there is a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc
- they model safe, responsible, and professional online behaviours in their own use of technology, including out of school and in their use of social media.

IT Provider

The DfE Filtering and Monitoring Standards says:
"Senior leaders should work closely with governors or proprietors, the designated safeguarding lead (DSL) and IT service providers in all aspects of filtering and monitoring. Your IT service provider may be a staff technician or an external service provider."

"Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The DSL should work closely together with IT service

providers to meet the needs of your setting. You may need to ask filtering or monitoring providers for system specific training and support."

"The IT service provider should have technical responsibility for:

- *providing and maintaining filtering and monitoring systems*
- *completing actions following concerns or checks to systems"*

"The IT service provider should work with the senior leadership team and DSL to:

- *procure systems*
- *identify risk*
- *carry out reviews*
- *carry out checks"*

The IT Provider is responsible for ensuring that:

- they are aware of and follow the school Online Safety Policy to carry out their work effectively in line with school policy
- the school technical infrastructure is secure and is not open to misuse or malicious attack
- the school meets (as a minimum) the required online safety technical requirements as identified by the DfE Meeting Digital and Technology Standards in Schools & Colleges and guidance from the local authority
- there is clear, safe, and managed control of user access to networks and devices
- they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- the use of technology is regularly and effectively monitored in order that any misuse / attempted misuse can be reported to the DSL for investigation and action

Pupils

- are responsible for using the school digital technology systems in accordance with the pupil Acceptable Use Policy and Online Safety Policy
- should understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- should know what to do if they or someone they know feels vulnerable when using online technology
- 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

Parents and Carers

Parents and carers play a crucial role in ensuring that their children understand the need to use the online services and devices in an appropriate way. The school will take every opportunity to help parents and carers understand these issues through:

- publishing the school Online Safety Policy on the school website
- providing them with a copy of the pupil Acceptable Use Policy
- publish information about appropriate use of social media relating to posts concerning the school
- seeking their permissions concerning digital images etc
- parents / carers evenings, newsletters, website, social media and information about national / local online safety campaigns and literature

Parents and carers will be encouraged to support the school in:

- reinforcing the online safety messages provided to pupils in school

4. Procedures

The DfE Keeping Children Safe in Education guidance suggests that:
"The breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas of risk:

Content: *being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.*

Contact: *being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.*

Conduct: *online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and nonconsensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying, and*

Commerce: *risks such as online gambling, inappropriate advertising, phishing and / or financial scams."*

The school will take all reasonable precautions to ensure online safety for all school users but recognises that incidents may occur inside and outside of the school (with impact on the school) which will need intervention. The school will ensure:

- there are clear reporting routes which are understood and followed by all members of the school community which are consistent with the school safeguarding procedures, and with our whistleblowing, complaints and managing allegations policies
- all members of the school community will be made aware of the need to report online safety issues / incidents
- that the School Business Manager regularly runs filtering and monitoring reports
- reports will be dealt with as soon as is practically possible once they are received
- the Designated Safeguarding Lead and other responsible staff have appropriate skills and training to deal with online safety risks
- if there is any suspicion that the incident involves any illegal activity or the potential for serious harm the incident must be escalated through the agreed school safeguarding procedures
- any concern about staff misuse will be reported to the headteacher, unless the concern involves the headteacher, in which case the complaint is referred to the Chair of Governors and the local authority
- it is important that those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively
- there are support strategies in place e.g., peer support for those reporting or affected by an online safety incident
- incidents should be logged on CPOMS
- relevant staff are aware of external sources of support and guidance in dealing with online safety issues, e.g. local authority, police, Professionals Online Safety Helpline, Reporting Harmful Content, CEOP
- those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions
- learning from the incident (or pattern of incidents) will be provided anonymously to:
  - staff, through regular briefings
  - pupils, through assemblies / lessons
  - parents / carers, through newsletters, school social media, website
  - governors, through regular safeguarding updates
  - local authority / external agencies, as relevant

5. Related Policies

The policies and guidance to help form safe environments to learn and work in include, but are not limited to the school's:

- Acceptable Use Policies (AUPs)
- Social Media Policy
- Photographic Images Policy
- Filtering & Monitoring Statement

These policies set the boundaries of acceptable use but are used in conjunction with, but not limited to:

- Behaviour Policy
- Anti-Bullying Policy
- Home School Agreements
- Staff Standards of Conduct
- Governors Code of Conduct