Wootton Bassett Infants' School

Online Safety Policy

Author:	WBIS
Approval Level:	HT
Issue Date/Last Amended	September 2026
Review Date:	October 2027
Review Cycle:	Annually

Introduction

The purpose of this policy statement is to:

- Ensure the safety and wellbeing of children and young people is paramount when adults, young people or children are using the internet, social media or mobile devices.
- Provide staff and volunteers with the overarching principles that guide our approach to online safety.
- Ensure that, as an organisation, we operate in line with our values and within the law in terms of how we use online devices.

The policy statement applies to all staff, volunteers, children and young people and anyone involved in Wootton Bassett Infants. This policy has been drawn up on the basis of legislation, policy and guidance that seeks to protect children in England.

The DfE Keeping Children Safe in Education statutory guidance requires Local Authorities, Multi Academy Trusts, and schools in England to ensure learners are safe from harm:

> *"It is essential that children are safeguarded from potentially harmful and inappropriate online material. An effective whole school and college approach to* ***online safety*** *empowers a school or college to protect and educate pupils, students, and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate".*
>
> *"Governing bodies and proprietors should ensure online safety is a running and interrelated theme whilst devising and implementing their whole school or college approach to safeguarding and related policies and procedures. This will include considering how online safety is reflected as required in all relevant policies and considering online safety whilst planning the curriculum, any teacher training, the role and responsibilities of the designated safeguarding lead (and deputies) and any parental engagement."*

The DfE Keeping Children Safe in Education guidance also recommends:

> ***Reviewing online safety*** *… Technology, and risks and harms related to it, evolve, and change rapidly. Schools and colleges should consider carrying out an annual review of their approach to online safety, supported by an annual risk assessment that considers and reflects the risks their children face.*

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, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, extremism, misinformation, disinformation (including fake news) and conspiracy theories.*

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 non-consensual 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. If you feel your pupils, students or staff are*

Schools in England are subject to an increased level of scrutiny of their online safety practices by Ofsted Inspectors during inspections, while the Counter Terrorism and Securities Act 2015 requires schools to ensure that children and young people are safe from terrorist and extremist material on the internet.

Rationale

We recognise that the online world provides everyone with many opportunities; however, it can also present risks and challenges. We have a duty to ensure that all children, young people and adults involved in our organisation are protected from potential harm online. We have a responsibility to help keep children and young people safe online, whether or not they are using school network and devices. Working in partnership with children, young people, their parents, carers and other agencies is essential in promoting young people's welfare and in helping young people to be responsible in their approach to online safety. All children, regardless of age, disability, gender reassignment, race, religion or belief, sex or sexual orientation, have the right to equal protection from all types of harm or abuse.

Aims

We believe that:

- Children and young people should never experience abuse of any kind.
- Children should be able to use the internet for education and personal development, but safeguards need to be in place to ensure they are kept safe at all times.

Objectives

We will seek to keep children and young people safe by:

- Appointing an online safety coordinator (Alison Pass- Designated Safeguarding Lead)
- Providing clear and specific directions to staff and volunteers on how to behave online through our Staff Behaviour policy.
- Supporting and encouraging the young people using our service to use the internet, social media and mobile phones in a way that keeps them safe and shows respect for others.
- Supporting and encouraging parents and carers to do what they can to keep their children safe online.
- Developing an online safety agreement for use with young people and their parents or carers

- Developing clear and robust procedures to enable us to respond appropriately to any incidents of inappropriate online behaviour, whether by an adult or a child or young person
- Reviewing and updating the security of our information systems regularly
- Ensuring that usernames, logins, email accounts and passwords are used effectively.
- Ensuring personal information about the adults and children who are involved in our organisation is held securely and shared only as appropriate.
- Ensuring that images of children, young people and families are used only after their written permission has been obtained, and only for the purpose for which consent has been given.
- Providing supervision, support and training for staff and volunteers about online safety
- Examining and risk assessing any social media platforms and new technologies before they are used within the organisation.

Assessment, Recording and Reporting

If online abuse occurs, we will respond to it by:

- Having clear and robust safeguarding procedures in place for responding to abuse (including online abuse).
- Providing support and training for all staff and volunteers on dealing with all forms of abuse, including bullying or cyberbullying, emotional abuse, sexting, sexual abuse and sexual exploitation.
- Making sure our response takes the needs of the person experiencing abuse, any bystanders and our organisation as a whole into account.
- Reviewing the plan developed to address online abuse at regular intervals, in order to ensure that any problems have been resolved in the long term.

Complaints of internet misuse will be dealt with by the Head Teacher and recorded. Any complaint about staff misuse will be reported to the Head Teacher. Complaints of a safeguarding nature must be reported to the named Designated Safeguarding Leads.

Filtering and Monitoring

The Department for Education's filtering and monitoring standards set out that schools should:

- identify and assign roles and responsibilities to manage filtering and monitoring systems.
- review filtering and monitoring provision at least annually.
- block harmful and inappropriate content without unreasonably impacting teaching and learning.
- have effective monitoring strategies in place that meet their safeguarding needs.

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 sections outline the online safety roles and responsibilities of individuals[1] 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, though the day-to-day responsibility for online safety is held by the Designated Safeguarding Lead, as defined in Keeping Children Safe in Education.
- The headteacher and (at least) another member of the senior leadership team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff[2].
- The headteacher/senior leaders are responsible for ensuring that the Designated Safeguarding Lead / Online Safety Lead, IT provider/technical staff, 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 receive regular monitoring reports from the Designated Safeguarding Lead / Online Safety Lead.
- The headteacher/senior leaders will work with the responsible Governor, the designated safeguarding lead (DSL) and IT service providers in all aspects of **filtering and monitoring.**

Governors

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

Governors will receive regular information about online safety incidents and monitoring reports. A member of the governing body will take on the role of Online Safety Governor to include:

- Regular meetings with the Designated Safeguarding Lead / Online Safety 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. (The review will be conducted by members of the SLT, the DSL, and the IT service provider and involve the responsible governor) - in-line with the DfE Filtering and Monitoring Standards
- Reporting to relevant *governors group/meeting*

- Receiving (at least) basic cyber-security training to enable the governors to check that the school meets the DfE Cyber-Security Standards

Designated Safeguarding Lead (DSL)

The DSL will:

- hold the lead responsibility for online safety, within their safeguarding role.
- Receive relevant and regularly updated training in online safety to enable them to understand the 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.
- meet regularly with the online safety governor to discuss current issues, review (anonymised) incidents and **filtering and monitoring** logs and ensure that annual (at least) **filtering and monitoring** checks are carried out.
- attend relevant governing body meetings/groups.
- report regularly to headteacher/senior leadership team
- be responsible for receiving reports of online safety incidents and handling them 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/OSL to develop a planned and coordinated online safety education programme.

This will be provided through:

- a discrete programme
- PHSE and RHE programmes
- A mapped cross-curricular programme
- Assemblies and pastoral programmes
- Through relevant national initiatives and opportunities e.g. ***Safer Internet Day*** and ***Anti-bullying week.***

Teaching and Support Staff

School staff are responsible for ensuring that:

- They have an awareness of current online safety matters/trends and of the current school Online Safety Policy and practices.
- They understand that online safety is a core part of safeguarding.
- They immediately report any suspected misuse or problem 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 rules.
- 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

If the school has a technology service provided by an outside contractor, it is the responsibility of the school to ensure that the provider carries out all the online safety measures that the school's obligations and responsibilities require. It is also important that the provider follows and implements school Online Safety Policy and procedures.

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 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 for investigation and action.
- the **filtering and monitoring** review is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person.
- monitoring systems are implemented and regularly updated as agreed in school policies.

Learners

- are responsible for using the school digital technology systems in accordance with the Online Safety rules.
- 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 rules cover 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 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
- publish information about appropriate use of social media relating to posts concerning the school.
- seeking their permissions concerning digital images, cloud services 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 learners in school.
- the safe and responsible use of their children's personal devices in the school (where this is allowed)

Teaching and Learning

Computing is used increasingly across the curriculum to enhance and extend learning, but it is essential that e-safety is an integral part of the delivery and use of computing equipment. Online safety is therefore embedded within the curriculum as follows:

- Online safety rules are introduced to the children at the start of each academic year.
- Online safety rules are re-visited on a regular basis within a range of curriculum areas including Personal, Social Health Education (PSHE).
- A set of internet rules are included for display in the classroom explaining how the children use the internet in school.
- Pupils are encouraged to tell a teacher immediately if they encounter any material that makes them feel uncomfortable.

Related Policies and Procedures

This policy statement should be read alongside our organisational policies and procedures, including:

- Safeguarding and Child Protection policy
- Anti-bullying policy and procedures
- Computing policy
- PSHE/RHE policy
- Behaviour and Discipline policy

Contact Details

Online safety co-ordinator

Name: Alison Pass (Headteacher and DSL)

Phone/email: head@woottonbassett-inf.wilts.sch.uk

Senior lead for safeguarding and child protection

Name: Alison Pass (Headteacher and DSL)

Phone/email: head@woottonbassett-inf.wilts.sch.uk

NSPCC Helpline 0808 800 5000