BY BROOK VALLEY CE PRIMARY SCHOOL

Online Safety Policy

Last Review Date: September 2026

Ratified By Governors Date: September 2026

Next Review Date: September 2027

Roots to grow, wings to fly
Growing, Flourishing, Soaring

Registered Address: By Brook Valley Academy Trust, The Street, Yatton Keynell, Wiltshire, SN14 7BA
Registered in England and Wales
Company Registration No. 8020467

Equality Impact Assessment (EIA) Part 1: EIA Screening

Policies, Procedures or Practices	Online Safety	Date	September 2026
EIA CARRIED OUT BY:	Foundation and Ethos	EIA APPROVED BY:	FGB

Groups that may be affected:

Are there any concerns that the policy could have a different impact on any of the following groups? (please tick the relevant boxes)	Existing or potential adverse impact	Existing or potential for positive impact
Age (young people, the elderly: issues surrounding protection and welfare, recruitment, training, pay, promotion)	Children may be too young to discern suitability of internet content	Children supervised appropriately according to age and ability
Disability (physical and mental disability, learning difficulties; issues surrounding access to buildings, curriculum and communication).		
Gender Reassignment (transsexual)		
Marriage and civil partnership		
Pregnancy and maternity		
Racial Groups (consider: language, culture, ethnicity including gypsy/traveller groups and asylum seekers		
Religion or belief (practices of worship, religious or cultural observance, including non-belief)		
Gender (male, female)		
Sexual orientation (gay, lesbian, bisexual; actual or perceived)		

Any adverse impacts are explored in a Full Impact Assessment.

By Brook Valley C of E VC Primary School

Online Safety Policy

Date: September 2026 Review Date: September 2027

Our Vision: Roots to grow, wings to fly

Growing, Flourishing, Soaring

The roots of our school community, based on our Christian values, nurture, help and support us to grow to be the best versions of ourselves. The wings of faith allow us to soar freely and flourish now and in the future

At By Brook Valley we are committed to creating a positive, safe and caring Christian environment, where all members of the school and wider community will be respected and valued. We support one another to put down strong roots within our distinctively Christian culture, growing from our core values of hope, honesty, forgiveness and friendship. In this way, we will each be the very best we can be. This policy should be read and understood from this perspective.

This Policy should be read in conjunction with:

• Child Protection Policy

• Positive Behaviour Policy

• Anti Bullying Policy

• RSHE Policy

• Code of Conduct for Safer Working Practice

• Responsible Use Policy (RUP)

- Mobile Phone Policy

Safeguarding Staff Behaviour Policy

Our online policy has been written by the school, building on the Wiltshire online template policy and government guidance. It has been agreed by the senior management, teachers and approved by governors through the Foundation and Ethos committee. It will be reviewed annually by the e- safety coordinator.

At By Brook Valley Primary school, we believe that:

- We have a duty to provide pupils with quality Internet access as part of their learning experience across all curricular areas. The use of the Internet is an invaluable tool in the development of lifelong learning skills.
- Used correctly Internet access will not only raise standards, but it will support teachers' professional work and it will enhance the school's management information and business administration systems.

We acknowledge that the increased provision of the Internet in and out of school brings with it the need to ensure that learners are safe. We need to teach pupils how to evaluate Internet information and to take care of their own safety and security.

It is essential that children are safeguarded from potentially harmful and inappropriate online material. An effective whole school approach to online safety empowers the school to protect and educate pupils, staff and parents in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate.

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 non-consensual sharing of nudes and semi-nudes and/ or pornography, sharing explicit images and online bullying, and

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

1.Leadership and Management

1.1 Authorised Access

Internet access for pupils should be seen as an entitlement on the basis of educational need and an essential resource for staff.

• The school receives Internet Service Provision (ISP) from Oakford Internet Services (OIS) and has a service which proactively monitors Internet usage.

• All staff and pupils are granted Internet access. A record will be kept up-to-date; for instance if a pupil's access is withdrawn.

• At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved online materials wherever possible.

• Parents will be informed that pupils will be provided with supervised Internet access

1.2 Filtering and Monitoring - Please refer to our Safeguarding and Child Protection Policy and KCSiE para 140-146

Despite careful design, filtering systems cannot be completely effective due to the speed of change of web content. Levels of access and supervision will vary according to the pupil's age. Internet access must be appropriate for all members of the school community from the youngest pupil to staff. Senior staff will regularly review filtering and monitoring reports from Oakford technology.

• The school will work in partnership with parents, Wiltshire Council, DfE and its ISP to ensure systems to protect pupils are reviewed and improved.

• If staff or pupils discover unsuitable sites, the URL (web address) and content must be reported to the Internet Service Provider via the online safety lead.

• Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

• Any material that the school believes is illegal or may place an individual at risk must be referred to the appropriate authorities i.e. Head teacher, Local Authority DoFA, Police, Internet Watch Foundation

1.3 Risk Assessment

As the quantity and breadth of the information available through the Internet continues to grow it is not possible to guard against every undesirable situation. The school will address the issue that it is difficult to remove completely the risk that pupils might access unsuitable materials via the school system.

• In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Wiltshire Council can accept liability for the material accessed, or any consequences of Internet access.

• Methods to identify, assess and minimise risks will be reviewed regularly.

• The Head teacher will ensure that the Internet policy is implemented and compliance with the policy monitored.

• The use or access of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

2.1 The Curriculum

The Internet is an essential resource to support teaching and learning. The statutory curriculum requires pupils to be responsible, competent, confident and creative users of information and communication technology. In delivering the curriculum, teachers need to plan to integrate the use of communications technology such as web-based resources, e-mail and mobile learning. Computer skills are vital to access life-long learning and employment; indeed, Computing is now seen as an essential life-skill.

• Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

• The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, ensure wellbeing, to support the professional work of staff and to enhance the school's management information and business administration systems.

• Whilst Internet access is an entitlement, users will need to show a responsible and mature approach to its use or this privilege may be removed.

• The Internet is an essential part of everyday life for education, business and social interaction. The school has a duty to provide students 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.

2.2 Enhancing Teaching and Learning

Benefits of using the Internet in education include:

• Access to a variety of worldwide educational resources.

• Inclusion in the National Education Network, which connects all UK schools.

• 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.

• Collaboration across networks of schools, support services and professional associations.

• Improved access to technical support including remote management of networks and automatic system updates.

• Access to learning wherever and whenever convenient.

2.3 Evaluating Content

Information received via the web, e-mail or text message requires good information-handling and digital literacy skills. In particular, it may be difficult to determine origin and accuracy, as the contextual clues may be missing or difficult to read. A whole curriculum approach has been adopted through the National Online Safety Programme. Ideally, inappropriate material would not be visible to pupils using the web but this is not easy to achieve and cannot be guaranteed. Pupils are taught what to do if they experience material that they find distasteful, uncomfortable or threatening.

• Pupils will be taught to be critically aware of the materials they read and how to validate information before accepting its accuracy.

• 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.

• If staff or pupils discover unsuitable site or content they consider to be inappropriate, the URL (address) and content should be reported to their ISP/OIS

• Schools should ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.

• Pupils will be taught to acknowledge the source of information used and to respect individuals and intellectual property when using Internet material in their own work.

3. Communication and Content

3.1 Website Content

Many schools have excellent websites that inspire pupils to publish work of a high standard. Publication of any information online should always be considered from a personal and school security viewpoint. Sensitive information may be better published in the school handbook or on a secure online area which requires authentication. Editorial guidance will help reflect the school's requirements for accuracy and good presentation.

• The point of contact on the school website should be the school address, school e-mail and telephone number. Staff or pupils' personal information will not be published.

• Written permission from individuals, parents or carers will be obtained before photographs of pupils are published on the school website. Photographs will be selected carefully and will not enable individuals to be clearly identified.

• Pupils' full names will not be used anywhere on the website, particularly in association with photographs.

• The nature of all items uploaded will not include content that allows the pupils to be identified, either individually or through aggregated pieces of information.

• The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

• The website should comply with the school's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.

3.3 Managing e-mail

E-mail is an essential means of communication for both staff and pupils. Directed e-mail use can bring significant educational benefits and interesting projects between schools. However, the use of e-mail requires appropriate safety measures. At present pupils do not have e-mail accounts at the school but should they be introduced then the following will apply. The use of e-mail identities such as john.smith@school.wilts.sch.uk will be avoided, as revealing this information could potentially expose a child to identification by unsuitable people.

• Pupils may only use approved e-mail accounts on the school system.

• Pupils must immediately tell a responsible adult if they receive offensive e-mail.

• Staff must use official school provided e-mail accounts for all professional communications.

• Pupils should use e-mail in an acceptable way. Sending images without consent, explicit images, messages that cause distress and harassment to others are considered significant breaches of school Responsible Use Policy (RUP) and will be dealt with accordingly.

• E-mail sent to an external organisation should be written carefully and where appropriate, authorised before sending, in the same way as a letter written on school headed paper.

3.4 On-line communications and Social Media.

On-line communications, social networking and social media services are filtered in school by the ISP but are likely to be accessible from home. All staff are made aware of the potential risks of using social networking sites or personal publishing either professionally with students or personally. They are made aware of the importance of considering the material they post, ensuring profiles are secured and how publishing unsuitable material may affect their professional status. All staff also read and sign a Responsible Use Policy. Pupils will be encouraged to think about the ease of uploading personal information, the associated dangers and the difficulty of removing an inappropriate image or information once published. Schools have a key role to teach young people about the importance of how to communicate safely and respectfully online, keeping personal information private. It is important that pupils are made aware of their options if they do make a mistake when sharing information on-line, and who they can talk to.

• Users are taught about how to keep personal information safe when using online services. Examples would include real name, address, photographs, mobile or landline phone numbers, school attended, IM and e-mail addresses, full names of friends/family, specific interests and clubs etc.

• Users must not reveal personal details of themselves or others in online communication, including the tagging of photos or video, or to arrange to meet anyone.

• Staff wishing to use Social Media tools with students as part of the curriculum will risk assess the sites before use and check the sites' terms and conditions to ensure the site is age appropriate. Staff will obtain documented consent from the Senior Leadership Team before using Social Media tools in the classroom.

• Staff official blogs or wikis should be password protected and only operate with approval from the SLT.

• 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 are advised on security and privacy online, including specific apps where appropriate e.g. Snapchat, Facebook or TikTok. Pupils are encouraged to set passwords, deny access to unknown individuals and to block unwanted communications. Pupils are encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private. Pupils are taught how to report inappropriate behaviour online and on apps, including how to block users.

• Pupils are taught about the risks of sharing photographs online, including over text message. Where appropriate, discussions about 'Sexting' – sending sexually explicit messages – will take place. Pupils are encouraged to behave respectfully when sharing photos of other people, making sure they always ask permission.

• No member of the school community should publish specific and detailed private thoughts about the school, especially those that may be considered threatening, hurtful or defamatory.

• Concerns regarding students' 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 students' underage use of sites. The school reserves the right to monitor its systems and communications in line with its rights under the Regulation of Investigatory Powers Act 2000.

• Disclosures from children regarding their use of social networking, social media or personal publishing (in or out of school) will be dealt with in line with the Child Protection, Anti-Bullying or Behaviour policies.

• 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 RUP.

• In line with, 'Guidance for Safer Working Practice for Adults who Work with Children and Young People' it will not be considered appropriate for staff to engage in personal online communications with children and young people, parents or carers. Express care is also to be taken regarding the use of social networking sites.

3.6 Mobile Devices (Including Bring You Own Device-BYOD)

For the purpose of this policy a mobile device is any device that provides access to the internet or internal network for example, mobile phone, tablet (iPad or similar), e-reader or wifi enabled digital camera. Mobile devices can be used to facilitate communication in a variety of ways with text, images, sound and internet accesses all common features. A policy which prohibits users from taking mobile devices to school could be considered to be unreasonable and unrealistic for schools to achieve. Due to the widespread use of mobile devices it is essential that the school take steps to ensure that these devices, both personally and school owned, are used responsibly. Allowing the use of mobile devices is a school decision, and will be subject to the following key principles:

• All individuals are protected from inappropriate material, bullying and harassment

• Users have access to resources to support learning and teaching

• Users will be given clear boundaries on responsible and professional use. The school operates the following procedures:

Visitors are required to hand in all mobile devices to the office upon arrival at school, or leave in Head's office, if they are going into classrooms or other parts of the school where children are present, including outside areas.

• Visitors are required to hand in all cameras (or any device with the ability to take photos or video) to the office upon arrival at school, or leave in Head's office, if they are going into classrooms or other parts of the school where children are present including outside areas.

• Staff are not permitted to use mobile phones in the classroom unless it is with the permission of the senior leadership team

• Staff will be provided with school equipment for taking photos or videos of pupils linked to an educational intention. In exceptional circumstances staff may need to use personal devices for such a purpose and when doing so, should ensure they comply with the school's Responsible Use Policy (RUP).

• For the safeguarding of all involved, users are encouraged to connect mobile devices through the school wireless provision and service that allows the ability to filter any device that uses the school Internet connection, without having to configure the user's device.

• The school will take steps to monitor responsible use in accordance with the Responsible Use Policy

• Parents wishing to photograph or video at an event should be made aware of the school's expectations and be required to comply with the schools RUP as a condition of permission to photograph or record

3.6 Video Conferencing

Video conferencing (including FaceTime, Skype, Zoom and Teams) enables users to see and hear each other between different locations. This 'real time' interactive technology has many potential benefits in education and where possible should take place using the school's wireless system.

• Staff must refer to any Responsible Use Policy or agreements prior to children taking part in video conferences.

• All video conferencing equipment in the classroom must be switched off when not in use and not set to auto answer.

• Pupils will ask permission from a teacher before making or answering a video conference call.

• Video conferencing is supervised appropriately for the pupil's age and ability.

3.7 Emerging Technologies

Many emerging communications technologies offer the potential to develop new teaching and learning tools, including mobile communications, Internet access, collaboration and multimedia tools. A risk assessment should be completed on each new technology and assessed for effective and safe practice in classroom use. The safest approach is to deny access until a risk assessment has been completed and safety has been established. Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

3.8 AI Usage

1. Purpose

This section outlines the responsible, ethical, and safe use of Artificial Intelligence (AI) technologies within the school environment. It applies to all staff, pupils, and parents engaging with AI tools for educational purposes.

2. Guiding Principles

Enhancement, not replacement: AI should support teaching, learning, and administration—not replace human judgement or relationships.

AI systems must be used in a manner that promotes equality, diversity and inclusion. Staff must consider the potential for bias within AI-generated outputs and ensure decisions affecting pupils are fair and non-discriminatory.

Safety first: All AI use must prioritise child safety, data protection, and compliance with UK law.

Transparency: AI-generated content must be clearly labelled and verified for accuracy.

3. Approved Use of AI

Staff Use:

- Lesson planning, resource creation, marking, and administrative tasks.

- Only school-approved AI tools may be used, accessed via school accounts.

Pupil Use:

- Age-appropriate, supervised activities such as creative writing, coding, or problem-solving.

- Use must be guided by staff and include digital literacy education.

4. Legal and Ethical Compliance

Adhere to UK GDPR and data protection laws.

Do not input personally identifiable or sensitive data into AI systems.

Respect intellectual property rights—no unauthorised use of copyrighted material.

5. Safeguarding and Risk Management

AI use must align with the school's safeguarding policies.

Any AI tool used by pupils must comply with the provider's age requirements and be approved by the school following safeguarding, security and data protection checks.

A Designated Safeguarding Lead (DSL) will oversee AI-related risks.

Conduct regular risk assessments and maintain an AI tool inventory.

6. Training and Awareness

Staff and governors will receive training on AI's benefits, risks, and ethical use.

Pupils will be taught to critically assess AI-generated content and understand its limitations.

7. Reporting and Accountability

Any misuse, data breaches, or inappropriate AI outputs must be reported immediately.

Clear reporting channels will be available for staff, pupils, and parents.

Disciplinary procedures will apply for policy violations.

8. Parent and Carer Engagement

Parents will be informed about AI use through newsletters, workshops, and online resources.

Feedback and concerns will be welcomed and addressed transparently.

9. **10. Governance**

The Headteacher and Governing Body retain overall responsibility for the school's use of AI. AI must not replace professional judgement or be used as the sole basis for decisions affecting pupils, staff, or families. New AI systems will be subject to appropriate safeguarding, security, equality and data protection assessments before implementation.

10. Monitoring and Review

This policy will be reviewed annually or in response to significant changes in AI technology or legislation.

The school will stay updated with DfE guidance and sector best practices.

3.9 Cyber Bullying

The Department for Education define cyber-bullying as an aggressive, intentional act carried out by a group or individual, using electronic forms of contact, repeatedly and over time against a victim who cannot easily defend him of herself

Cyber bullying can include:

- excluding a child from online games, activities or friendship groups
- sending threatening, upsetting or abusive messages

- creating and sharing embarrassing or malicious images or videos
- 'trolling' - sending menacing or upsetting messages on social networks, chat rooms or online games
- voting for or against someone in an abusive poll
- setting up hate sites or groups about a particular child
- creating fake accounts, hijacking or stealing online identities to embarrass a young person or cause trouble using their name.

For most, using the internet and mobile devices is a positive and creative part of their everyday life. Unfortunately, technologies can also be used negatively. It is essential that young people, school staff, parents and carers understand how cyber bullying is different from other forms of bullying, how it can affect people and how to respond and combat misuse. Promoting a culture of confident users will support innovation and safety. Cyber bullying (along with all other forms of bullying) of or by any member of the school community will not be tolerated. Full details are set out in the school's behaviour, anti-bullying and child protection policies, which should include:

• Clear procedures set out to investigate incidents or allegations of cyber bullying.

• Clear procedures in place to support anyone in the school community affected by cyber bullying.

• All incidents of cyber bullying reported to the school will be recorded.

• 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 ISP and the police, if necessary.

• Pupils, staff and parents/carers will be required to work with the school to support the approach to cyber bullying and the school's Online Safety ethos.

3.10 Data Protection

The quantity and variety of data held on pupils, families and on staff is expanding quickly. While this data can be very useful in improving services, data could be mishandled, stolen or misused. The Data Protection Act 1998 gives individuals the right to know what information is held about them and provides a framework to ensure that personal information is handled properly. It promotes openness in the use of personal information. Schools will already have information about their obligations under the Act; this section is a reminder that all data from which people can be identified is protected. For advice and guidance relating to a contravention of the Act, contact www.wiltshire.gov.uk

• Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

4 Implementation

4.1 Policy in Practice - Pupils

Many pupils are very familiar with Internet use and the culture that surrounds it. As part of the school's Online Safety teaching and awareness-raising it is important to discuss the key features with pupils as appropriate for their age. Pupils may need to be reminded of the school rules at the point of Internet use.

• All users will be informed that network and Internet use will be monitored.

• Online Safety teaching is integral to the curriculum and the school will raise the awareness and importance of safe and responsible internet use amongst pupils.

• Online Safety teaching is included in RSHE, Citizenship and Computing, and covers safe use at school and home.

• Online Safety rules will be on display in all rooms with Internet access.

• Safe and responsible use of the Internet and technology is reinforced across the curriculum and subject areas.

4.2 Policy in Practice - Staff

It is important that all staff feel confident to use new technologies in teaching and the School Online Safety Policy will only be effective if all staff subscribe to its values and methods. Staff should be given opportunities to discuss the issues and develop appropriate teaching strategies. Particular consideration must be given when members of staff are provided with devices by the school, which may be accessed outside the school network. Schools must be clear about the safe and appropriate uses of their school provided equipment and have rules in place about use of the equipment by third parties. Staff must be made aware of their responsibility to maintain confidentiality of school information. If a member of staff is concerned about any aspect of their ICT or internet use either on or off site, they should discuss this with their senior leader to avoid any possible misunderstanding.

• The Online Safety Policy will be provided to and discussed with all members of staff and Responsible Use Policy signed for compliance.

• Staff should be aware that Internet traffic is monitored by OIS and can be 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, is provided for all members of staff.

• All members of staff are 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.

4.3 Policy in Practice - Parents

Parents need to be aware of the potential dangers that are associated with online communications, social networking sites and mobile technologies to help ensure their children are not putting themselves at risk.

• Parents' attention will be drawn to the Online Safety Policy and Responsible Use Policy (RUP) in newsletters, school prospectus and Website.

• A partnership approach with parents will be encouraged. This could include offering parent evenings, demonstrations, practical sessions and suggestions for resources and safer Internet use at home.

• Regular information will be provided to parents about how to ensure they can work with the school to ensure this resource is used appropriately both within school and home. These can be accessed through the school website.

• Internet issues will be handled sensitively to inform parents without undue alarm.

• Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.

4.4 Handling of complaints

Parents and teachers must know how and where to report incidents in line with the school complaints policy and complaints of a child protection nature must be dealt with in accordance with the LA Child Protection

procedures. Prompt action will be required if a complaint is made. The facts of the case will need to be established; for instance whether the Internet use was within or outside school. A minor transgression of the rules may be dealt with by the teacher as part of normal class discipline. Other situations could potentially be serious and a range of sanctions will be required, linked to the school's behaviour policy. All records of the incident should be kept, e.g. e-mails saved or printed, text messages saved etc.

• Responsibility for handling incidents will be delegated to a senior member of staff.

• Any complaint about staff misuse must be referred to the head teacher.

• Pupils and parents will be informed of the complaints procedure.

• Parents and pupils will need to work in partnership with staff to resolve issues.

• There may be occasions when the police must be contacted. Early contact could be made to establish the legal position and discuss strategies.

5 Reviewing online safety

Technology, and risks and harms related to it, evolve, and change rapidly. The school carries out an annual review of their approach to online safety, supported by an annual risk assessment that considers and reflects the risks pupils face. This annual review will be carried out by the online safety lead and reported to the Head teacher and Foundation and Ethos Governing body.

6 Roles and responsibilities

6.1 The Governing Body has:

- delegated powers and responsibilities to the Head teacher to ensure all school personnel and stakeholders are aware of and comply with this policy;
- responsibility for ensuring this policy and all policies are maintained and updated regularly;
- made effective use of relevant research and information to improve this policy;
- responsibility for ensuring policies are made available to parents;
- undertaken training in order to understand Online Safety issues and procedures;
- nominated a link Safeguarding governor to:
    a) visit the school regularly;
    b) work closely with the Head teacher and the coordinator;
    c) ensure this policy and other linked policies are up to date;
    d) ensure that everyone connected with the school is aware of this policy;
    e) attend training related to this policy;
    a) annually report to the Governing Body on the success and development of this policy.

6.2 The role of the Head teacher

The Head teacher will:

b) ensure the safety and Online Safety of all members of the school community;
c) work in conjunction with the Senior Leadership Team to ensure all school personnel, pupils and parents are aware of and comply with this policy;
d) appoint a member of staff to be responsible for Online Safety;
e) work closely with the Governing Body and the coordinator
f) ensure risk assessments are in place
g) ensure regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable;
h) embed Online Safety in all aspects of the curriculum and other school activities;

i) investigate, record and report all infringements to Online Safety by any member of the school personnel or by a pupil;
j) deal with all complaints of Internet misuse by school personnel or pupils;
k) inform parents if their child has misused the Internet;
l) deal with all breaches of security;
m) impose the appropriate sanctions to any infringement of Online Safety;
n) will immediately suspend a member of the school personnel if they commit an exceptionally serious act of gross misconduct;
o) will immediately suspend and report to the Police if images of child abuse are found on a computer belonging to a member of the school personnel;
p) ensure any inappropriate websites or material found by pupils or school personnel will be reported to the Online Safety Coordinator who in turn will report to the Internet Service Provider;
q) ensure the school website complies with current DfE guidelines;
r) work closely with the link governor and coordinator;
s) provide guidance, support and training to all staff;
t) ensure parents/ carers are kept up to date with latest guidance, training and support
u) monitor the effectiveness of this policy and the curriculum through the Online Safety coordinator.

6.3 Role of the online safety coordinator/DSL

The coordinator will:

- be responsible for the day-to-day online safety issues;
- ensure that all Internet users are kept up to date with new guidance and procedures;
- ensure regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable;
- report any incidents to the Headteacher;
- ensure online safety is embedded in all aspects of the curriculum and other school activities;
- provide information and guidance for parents/carers in order to:
- increase their understanding of the internet;
- discuss the serious safeguarding issues and risks for children online and how to keep them safe;
- regularly update the school website with online safety information for parents and carers;
- develop a progressive online safety curriculum for the whole school;
- lead the development of this policy throughout the school;
- work closely with the Head teacher and the nominated governor;
- make effective use of relevant research and information to improve this policy;
- provide guidance and support to all staff;
- provide training for all staff on induction and when the need arises;
- keep up to date with new developments and resources;
- complete an annual review of online safety, including the success and development of this policy and report to the Foundation and Ethos committee and Head teacher.