Box CE VC Primary School
Online Safety Policy

This policy is based on the '360safe School online safety policy Sept 2023. This policy should be read in conjunction with other related policies and procedures e.g.

- Child protection policy
- Child protection procedures and record keeping
- Behaviour policy
- Anti-bullying policy
- Disability and equality scheme
- Whistleblowing policy
- Data Protection Policy
- Computing policy
- Responsible Use of the Internet policy for children
- Acceptable Use of the Internet policy for staff
- Child-Friendly Online safety policy
- Laptop policy for staff
- iPad policy for staff
- Personal Use of Social Media for Staff and Governors policy

Rationale

This online safety policy outlines the commitment of Box Primary School to safeguard members of our school community online in accordance with statutory guidance and best practice. The internet has become an important aspect of everyday life and children need to be able to use it safely and responsibly. We believe that the internet offers a valuable resource for teachers and children, as well as providing new ways to communicate with others worldwide.

This online safety 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 (where allowed).

Policy and Responsibilities

1. Leadership and Management

The leadership and management team ensure the online safeguarding of members of our school community. It is important that all members of the community work together to develop safe and responsible online behaviours, learning from each other, 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 and groups within the school.

Written	This Review	Next Review
September 2023		September 2026

- 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. The day-to-day responsibility for online safety is held by the Designated Safeguarding Lead (DSL), as defined in Keeping Children Safe in Education.
- The headteacher and online safety lead (OSL) should be aware of the procedures to be followed in the event of a serious online safety allegation.
- The headteacher, OSL, IT Provider and other relevant staff carry a responsibility to ensure they receive suitable training to enable them to carry out their roles and train others colleagues.
- The headteacher and OSL will monitor the incident log and ensure support is in place for following the incident flow chart.
- The headteacher/senior leaders will work with the responsible governor, the designated safeguarding lead (DSL) and IT service provider in all aspects of filtering and monitoring.
- The OSL will have a leading role in establishing and reviewing the school online safety policies/ documents.
- The headteacher and OSL will liaise with curriculum leaders and ensure that the online safety curriculum is planned, mapped, embedded and evaluated.

1.2 Governors

Governors are responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy.

This review will be carried out by the (*insert name of governor group/committee*) whose members 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 DSL / OSL
- 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 relevant *governors group/meeting*.

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

1.3 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 immediately report any suspected misuse or problem to the DSL and OSL for investigation/action, in line with the school safeguarding procedures

- all digital communications with pupils and parents/carers are on a professional level *and only carried out using official school systems*
- ensure pupils understand and follow the online safety policy and acceptable use agreements, have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- 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 pupils are guided to sites checked as suitable for their use
- where lessons take place using live-streaming or video-conferencing, there is regard to national safeguarding guidance and local safeguarding policies
- 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.

1.4 IT Provider and technical staff

The DfE Filtering and Monitoring Standards says:

"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."

It is the responsibility of our school to ensure that the provider carries our all the online safety measures that the school's obligations and responsibilities require. The IT provider and support staff will also follow and implement the school online safety policy and procedures.

1.5 Pupils

- Are responsible for using the school digital technology systems in accordance with the learner acceptable use agreement 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.

1.6 Parents and Carers

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 pupils' acceptable user agreement
- publish information about appropriate use of social media relating to posts concerning the school
- seeking their permissions concerning digital images, cloud services etc
- providing parents'/carers' evenings, newsletters, website and information about national/local online safety campaigns and literature.

2. Online Safety Committee

The online safety committee has a wide representation from the school community, with responsibilities for issues regarding online safety and monitoring the online safety policy and its impact. The committee will also be responsible for reporting to senior leaders and the governing body.

The online safety committee has the following members:

- OSL
- online safety governor
- a representative from each year group from year 1 upwards.

Members of the Online Safety Group will assist the DSL and OSL with:

- the reviewing and monitoring of the online safety policy
- the production and monitoring of the Child Friendly Online Safety Leaflet
- encouraging the contribution of pupils to staff awareness, emerging trends and the school online safety provision
- monitoring improvement actions identified through use of the 360-degree safe self-review tool
- learners contribute to the online safety education programme e.g. peer education, digital leaders leading lessons for younger pupils, online safety campaigns
- pupils designing/updating acceptable use agreements
- contributing to online safety events with the wider school community e.g. parents' evenings, family learning programmes etc.

3. Reporting and Responding

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 the whistleblowing and complaints policy

- all members of the school community will be made aware of the need to report online safety issues/incidents
- reports will be dealt with as soon as is practically possible once they are received
- the DSL, OSL 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
- incidents will be logged
- staff will be aware of external support and guidance with online safety issues, e.g. local authority; police
- those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions.

3.1 How will the risks be assessed?

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. However, the school will address the issue that it is difficult to completely remove 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. Box Primary 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 or Wiltshire Council can accept liability for the material accessed, or any consequences of internet access. It is important to remember that the use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990. We will regularly review methods to identify, assess and minimise risks. The head teacher will ensure that the policy is implemented and that compliance with the policy is monitored.

4. Teaching and learning

4.1 Why is internet use important?

The internet is an essential resource to support teaching and learning. The curriculum requires pupils to learn how to locate, retrieve and exchange information using ICT. In delivering the curriculum, teachers need to plan to integrate the use of communications technology such as web-

based resources and email and mobile learning. Computer skills are vital to access life-long learning and employment; indeed, computing is now seen as an essential life-skill.

The purpose of internet use in school is to raise educational standards, to promote pupil achievement, well-being and to support the professional work of staff and to enhance the school's management information and business administration systems. The internet is an essential part of everyday life for education, business and social interaction. Our school has a duty to provide students with quality internet access as part of their learning experience. 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. It is also important to remember that 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.

4.2 How will internet use enhance learning?

Using the internet in education has many benefits including:

- access to worldwide educational resources including museums and art galleries
- 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.

4.3 Education programme

Online safety is a focus in all areas of the curriculum and staff reinforce online safety messages across the curriculum. The online safety curriculum is broad, relevant and provides progression, with opportunities for creative activities and is provided in the following ways:

- a planned online safety curriculum for all year groups matched against the nationally agreed framework SWGfL Project Evolve and regularly taught in a variety of contexts
- lessons are matched to need; are age related and build upon prior learning
- lessons are relevant with agreed objectives leading to clear outcomes
- incorporates and makes use of national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week
- online safety and digital competency is threaded through other curriculum areas e.g. PSHE; English etc.

- the online safety curriculum is relevant and up to date to ensure the quality of learning and outcomes.

Through Online safety education, pupils will learn:

- to be critically aware of the materials they read and shown how to validate information before accepting its accuracy
- to use age-appropriate tools to research internet content
- to acknowledge the source of information used and to respect copyright when using internet material in their own work
- to use social networking responsibly and respectfully
- how to keep their personal information private and to create secure passwords
- how to report problems and deal with unwanted communications
- how to share information safely and responsibly.

4.4 Staff training

All staff will receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- the training will be an integral part of the school's annual safeguarding and data protection training for all staff
- all new staff will receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and acceptable use agreements. It includes explicit reference to classroom management, professional conduct, online reputation and the need to model positive online behaviours.

4.5 Governor training

Governors will take part in online safety training/awareness sessions such as **NSPCC** E-safety training www.nspcc.org.uk

A higher level of training will be made available to the online safety governor.
This will include:

- cyber security training (at a basic level)
- training to allow the governor to understand the school's filtering and monitoring provision, in order that they can participate in the required checks and review.

4.6 Family training

Parents and carers play a crucial role in the education of their children and in monitoring/regulation of their children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will provide information and awareness to parents and carers through:

- the school website which is used to promote a number of online safety resource websites that parents can use at home with their children
- publishing the Online safety policy on the school website
- providing them with a copy of the pupils' acceptable use agreement
- giving them the opportunity to take part in every other year parent online safety learning sessions
- our school newsletter, regular information is provided to parents about how to ensure they can work with the school to use this resource is used appropriately both within school and home
- handling internet issues sensitively to inform parents without undue alarm
- advice on filtering systems and educational and leisure activities that include responsible use of the internet are available to parents
- all parents are aware of who the computing subject leader is and will receive support information termly from the subject leader e.g. Know It All for Parents.

5. Technology

The school is responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. The school ensures all staff are made aware of policies and procedures in place on a regular basis and explain that everyone is responsible for online safety and data protection.

Box Primary School has an external service provider (EFX Solutions). It is the responsibility of the school to ensure the provider carries out all the online safety and security measures that would otherwise be the responsibility of the school.

6. Filtering and Monitoring

The school filtering and monitoring provision is agreed by senior leaders, governors and the IT Service Provider and is regularly reviewed (at least annually) and updated in response to changes in technology and patterns of online safety incidents/behaviours.

Checks on the filtering and monitoring system are carried out by the IT Service Provider in consultation with the DSL.

Through Broadband4 the school has managed internet access which offers a fully granular filtering solution integrated with a premises directory services platform. This granularity allows filtering rules to be deployed down to an individual user level, rather than by groups, virtual local area network (VLAN) or Subnet. All Broadband4 customers have access to their own Web Filtering control panel allowing them to manage filtering rules themselves making changes instantly. These changes do however need to be agreed with the DSL and IT service provider.

- The school manages access to content across its systems for all users and on all devices using the school's internet provision (Broadband4). The filtering provided is built to exceed the standards defined in the DfE Filtering standards for schools and colleges and KSCIE.
- Illegal content (e.g. child sexual abuse images) is filtered by Broadband4 by actively employing the Internet Watch Foundation URL list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. Content lists are regularly updated.
- There are established and effective routes for users to report inappropriate content, recognising that no system can be 100% effective.
- Filtering logs are regularly reviewed and alert the Designated Safeguarding Lead to breaches of the filtering policy, which are then acted upon.

6.1 Monitoring

The school has monitoring systems in place to protect the school, systems and users:

- the school monitors all network use across all its devices and services
- monitoring reports are urgently picked up, acted on and outcomes are recorded by the Designated Safeguarding Lead, all users are aware that the network (and devices) are monitored
- there are effective protocols in place to report abuse/misuse. There is a clear process for prioritising response to alerts that require rapid safeguarding intervention
- management of serious safeguarding alerts is consistent with safeguarding policy and practice.

7. Communication and Content

7.1 The School Website

The school communicates with parents/carers and the wider community and promotes the school through:

- public-facing website
- online content in newsletters.

The school ensures the online safety policy has been followed in the use of online publishing. The point of contact on the website is the school address, school email and telephone number. Staff or pupils' home information will not be published. Where learner work, images and videos are published, their identities are protected, and full names are not published. Written permission from parents or carers will be obtained before photographs, audio or videos of pupils are published on the school website.

7.2 Managing email

Email is an essential means of communication for both staff and pupils. Directed email use can bring significant educational benefits and interesting projects between schools. However, the use of email requires appropriate safety measures. We do not give children personal use of email

identities such as john.smith@box.wilts.sch.uk as revealing this information could potentially expose a child to identification by unsuitable people. Pupils should not use personal email addresses in school. However, if a lesson requires the children to use email, it should be strictly monitored by the teacher and using an approved email account on the school system.

Pupils must immediately tell a responsible adult if they receive offensive email. Pupils should use email in an acceptable way. Sending images without consent, messages that cause distress and harassment to others are considered significant breaches of school conduct and will be dealt with accordingly.

- When sending emails, children should be referred to by their initials. Any sensitive documents sent by email should by password protected.
- All users have responsibility for the security of their username and password and must not allow other users to access the systems using their log on details.
- Emails must be accessed on a school device
- *NB: support staff who don't have a school device may access generic emails on a personal device. No information about staff or children should be sent from a personal device.*

7.3 Mobile technologies

The school acceptable use agreements for staff, pupils, parents, and carers outline the expectations around the use of mobile technologies.

The school allows:

	School devices			**Personal devices**		
	School owned for individual use	School owned for multiple users	Authorised device[1]	Student owned	Staff owned	Visitor owned
Allowed in school	**Yes**	**Yes**	**Yes**	Yes/No	Yes	Yes
Full network access	Yes	Yes	Yes	No	No	No
Internet only					Yes	Yes
No network access				Yes		

Children strongly discouraged to bring mobile devices into school unless there is a clear reason for them needing to and their parents inform the school. Mobile devices must be turned off and not taken out of their bags until off of the school premises. The children will be responsible for

its safekeeping. School staff may confiscate a mobile phone or device if the children do not follow the above information. If it is suspected that material contained on the device relates to a criminal offence, it will be handed over to the police for investigation. Any electronic devices that are brought in to school are the responsibility of the user. Our school accepts no responsibility for the loss, theft or damage of such items.

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 or informal capacity. Staff must 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. Staff must not use personal devices for any school business.

Staff should only use their mobile phones or other personal devices in designated breaks. Staff are responsible for their own devices at all times.

7.4 Online communications, social networking and social media

Online communications, social networking and social media services are filtered in school by Broadband4 but are likely to be accessible from home and on mobile devices.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils through:

- ensuring that personal information is not published
- education/training being provided including acceptable use, age restrictions, social media risks, digital and video images policy, checking of settings, data protection and reporting issues
- clear reporting guidance, including responsibilities, procedures, and sanctions
- guidance for pupils, parents/carers.

School staff should ensure that:

- no reference should be made in social media to pupils, parents/carers or school staff
- they do not engage in online discussion on personal matters relating to members of the school community
- personal opinions should not be attributed to the school
- security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information
- they act as positive role models in their use of social media
- staff/class official blogs are password protected and run with approval from the SLT.

Pupils will be taught and ensure that:

- pupils will be taught about how to keep personal information safe when using online services. Examples would include real name, address, mobile or landline phone numbers,

school attended, IM and email addresses, full names of friends/family, specific interests and clubs etc.

- pupils must not reveal personal details of themselves or others in online communication, or arrange to meet anyone
- personal publishing will be taught via age appropriate sites that are suitable for educational purposes. These are moderated by the school where possible
- pupils are advised on security and privacy online and 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
- 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.

7.5 Digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and pupils are made aware of the risks associated with publishing digital images on the internet.

The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- the school may use live-streaming or video-conferencing services in line with national and local safeguarding guidance / policies
- when using digital images, staff will inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images
- staff/volunteers must be aware of those pupils whose images must not be taken/published. Those images should only be taken on school devices.

7.6 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. Access of new technologies will be denied until they have been deemed appropriate by the SLT. They will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

7.7 Cyberbullying

Many young people and adults find that using the internet and mobile phones 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 and parents and carers understand how cyberbullying 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.

Cyberbullying is bullying that takes place using electronic technology. Electronic technology includes devices and equipment such as cell phones, computers, and tablets as well as communication tools including social media sites, text messages, chat, and websites.

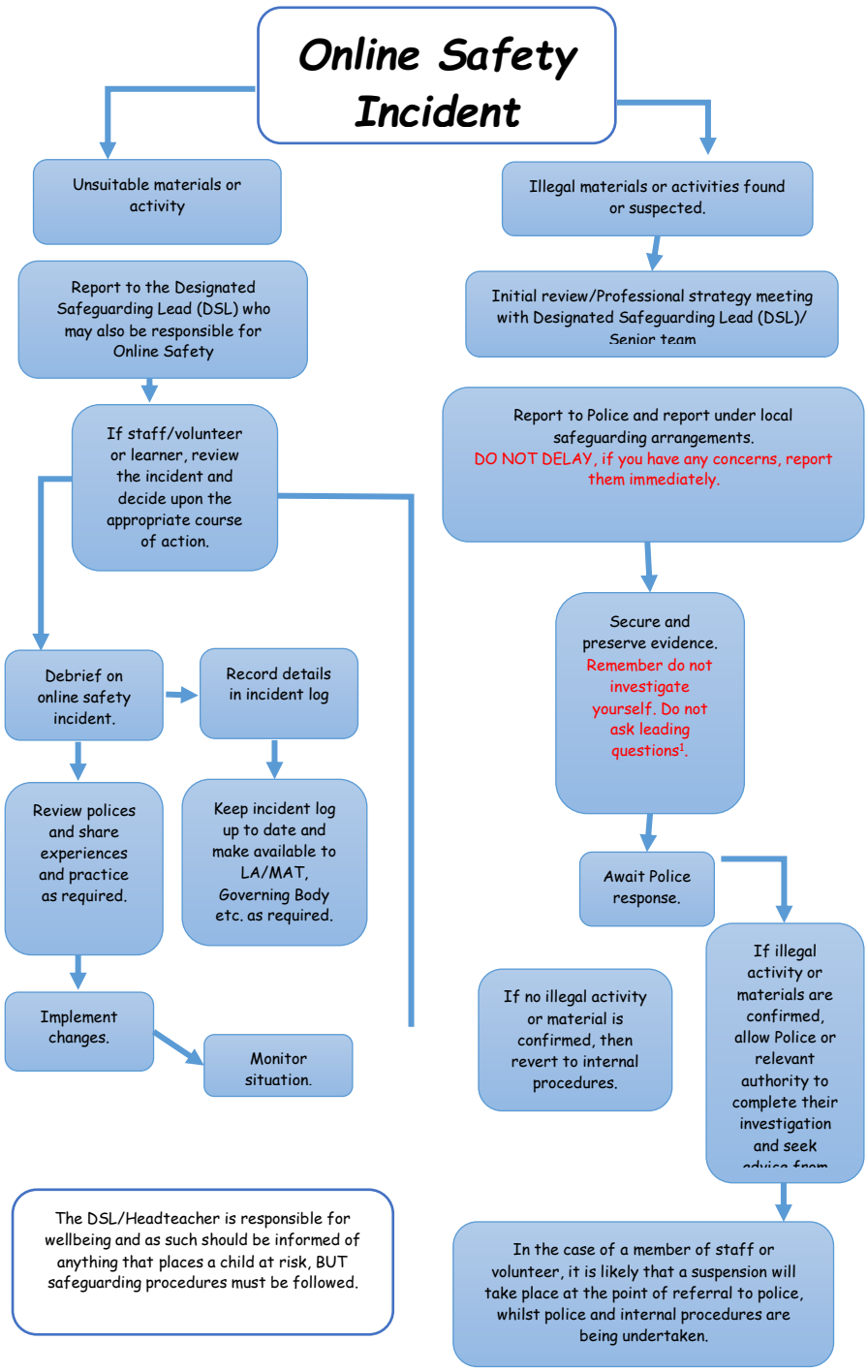
Examples of cyberbullying include nasty text messages or emails, rumours sent by email or posted on social networking sites, and embarrassing pictures, videos, websites, or fake profiles.

Cyberbullying can be defined as:
'…**'virtual' bullying, which can occur in or outside school. Cyber-bullying is a different form of bullying and can happen at all times of the day, with a potentially bigger audience, and more accessories as people forward on content at a click.**' DfE 2014

DfE and Childnet have produced resources and guidance that can be used to give practical advice and guidance on cyberbullying: http://www.digizen.org/cyberbullying

- 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.
- Incidents or allegations of cyberbullying will be investigated following the procedures outlined the anti-bullying policy whether they occur inside or outside school.
- Anyone in our school community who is affected by cyberbullying will be supported in accordance with the anti-bullying policy.
- All incidents of cyberbullying reported to the school will be recorded.
- The school will take steps to identify the bully, where possible and appropriate. This includes examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- Pupils, staff and parents/carers are required to work with the school to support the approach to cyberbullying and the school's online safety ethos.

Online Safety Incident



Additional resources and links:
Internet Watch Foundation: Report Child Sexual Abuse Images & Videos Online (iwf.org.uk)
Childline: Report Remove | Childline

Written	This Review	Next Review
September 2023		September 2026