

# ***ETTINGTON C of E PRIMARY SCHOOL***



*Learning for Fullness of Life*  
*Trust-Respect - Love*

---

## **ONLINE SAFETY POLICY**

Date of publication: December 2024

Review date: December 2025

## Ettington C of E Primary School

### CONTENTS

1. Aims .....	2
2. Legislation and guidance .....	3
3. Roles and responsibilities .....	3
4. Educating pupils about online safety .....	5
5. Engagement with parents and carers .....	6
6. Cyber-bullying .....	7
7. Managing information systems .....	9
8. Use of mobile phones and personal devices .....	11
9. How the school will respond to issues of misuse .....	12
10. Training .....	13
11. Monitoring arrangements .....	14
12. Links with other policies .....	14
Appendix 1: Acceptable Use Policy .....	15

### 1. AIMS

As a school, we aspire to live out God’s plan for all to flourish.

We believe in providing our children with opportunities to use and develop the gifts and talents they have been blessed with, to ensure they embrace ‘Life in its fullness’ (John 10:10) following the teachings of Jesus.

Our vision is to place the child at the heart of everything we do, ‘Learning for the Fullness of Life’. It is to work together, where everyone is a partner in learning; providing a safe, happy, caring and stimulating community, where children are given opportunities to reach their true potential.

At Ettington Church of England Primary School we believe that online safety (previously referred to as e-Safety) is an essential element of safeguarding children and adults in the digital world, when using technology such as computers, mobile phones or games consoles.

We appreciate that the internet, social media and information communication technologies are an important part of everyday life for many children, so our pupils must be supported to develop strategies to manage and respond to risk so they can be empowered to build their resilience and make sensible, informed choices when online.

We recognise that we have a duty to provide the school community with quality Internet access to raise education standards, promote pupil achievement, support professional work of staff and enhance the school’s management functions. We also acknowledge that, alongside this, there is a clear duty to ensure that children are protected from potential harm online.

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors.
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as ‘mobile phones’).
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

- Embrace the opportunity to build on learning, participating in Safer Internet Day during February.

### **The 4 key categories of risk**

Our approach to online safety is based on addressing the following categories of risk:

**Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism.

**Contact** – being subjected to harmful online interaction with other users, such as 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** – personal online behaviour that increases the likelihood of, or causes, harm, such as 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.

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

## **2. LEGISLATION AND GUIDANCE**

This policy is based on the Department for Education’s (DfE’s) statutory safeguarding guidance, [Keeping Children Safe in Education](#), and its advice for schools on:

[Teaching Online Safety in School’s](#)

[Preventing and Tackling Bullying](#)

[Relationships and Sex Education](#)

[Searching, Screening and Confiscation guidance](#)

It also refers to the DfE’s guidance on [protecting children from Radicalisation](#)

It reflects existing legislation, including but not limited to the [Education Act 1996](#) (as amended), the [Education and Inspections Act 2006](#) and the [Equality Act 2010](#). In addition, it reflects the [Education Act 2011](#), which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils’ electronic devices where they believe there is a ‘good reason’ to do so.

The policy also considers the National Curriculum computing programmes of study.

## **3. ROLES AND RESPONSIBILITIES**

### **3.1 The Governing Board**

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governor who oversees online safety is Heather Fletcher as part of her responsibility for safeguarding.

All governors will:

Ensure that they have read and understand this policy:

- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet.
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole school approach to safeguarding and related policies and/or procedures.
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable.

### **3.2 The Headteacher**

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

### **3.3 The Designated Safeguarding Lead**

Details of the school's designated safeguarding lead (DSL) and deputies are set out in our child protection and safeguarding policy as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Ensuring that staff understand this policy and that it is being implemented consistently throughout the school.
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents.
- Managing all online safety issues and incidents in line with the school child protection policy.
- Ensuring that any online safety incidents are logged on CPOMs and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are logged on CPOMs and dealt with appropriately in line with the school behaviour policy.
- Updating and delivering staff training on online safety.
- Liaising with other agencies and/or external services if necessary.
- Providing regular reports on online safety in school to the governing board.

This list is not intended to be exhaustive.

### **3.4 The IT Technical Support**

The IT technical support team are responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material.
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly.
- Conducting a full security check and monitoring the school's ICT systems on a frequent and regular basis.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files with the aid of Smoothwall.

- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet and ensuring that pupils follow the school's terms on acceptable use (appendices 1, 2 and 3)
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Always screen everything ahead of time, before lesson time.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

### **3.6 Parents**

Parents are expected to:

- Notify a member of staff or the Headteacher of any concerns or queries regarding this policy.
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet.

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – [UK Safer Internet Centre](#)
- Hot topics – [Childnet International](#)

### **3.7 Visitors and Members of the Community**

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use.

## **4. EDUCATING PUPILS ABOUT ONLINE SAFETY**

Pupils will be taught about online safety as part of the curriculum:

In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private.
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

Pupils in **Key Stage 2** will be taught to:

- Understand the dangers of not being safe online.
- Use technology safely, respectfully and responsibly.

- Recognise acceptable and unacceptable behaviour.
- Identify a range of ways to report concerns about content and contact .

By the **end of primary school**, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not.
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous.
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them.
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met.
- How information and data is shared and used online.
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context.)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know.

The safe use of social media and the internet will also be covered in other subjects where relevant, such as PSHE.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND to ensure that it is accessible for all pupils.

At Ettington, we recognise that parents and carers have an essential role to play in enabling children to become safe and responsible users of the internet and digital technology and will seek to engage with them about this in a variety of ways:

- Parents' attention will be drawn to the school Online Safety Policy and expectations in newsletters, letters, the school prospectus and on the school website.
- A partnership approach to online safety at home and at school with parents will be encouraged. This may include offering parent information evenings with demonstrations and suggestions for safe home Internet use or highlighting online safety at other well attended events e.g. parent evenings, transition events, fetes and sports days.
- All members of the school/setting community will be informed about the procedure for reporting online safety (e-Safety) concerns (such as breaches of filtering, cyberbullying, illegal content etc).
- The Designated Safeguarding Lead (DSL) will be informed of any online safety (e-Safety) incidents involving child protection concerns, which will then be recorded.
- The Designated Safeguarding Lead (DSL) will ensure that online safety concerns are escalated and reported to relevant agencies in line with the Warwickshire Safeguarding Children Board thresholds and procedures.
- Complaints about Internet misuse will be dealt with under the school's complaints procedure.
- Complaints about online bullying will be dealt with under the school's anti-bullying policy and procedure.
- Any complaint about staff misuse will be referred to the Headteacher.
- Any allegations against a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer).
- Parents and staff will be informed of the school's complaints and whistleblowing procedures.
- All members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns.

- All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community.
- The school will manage online safety (e-Safety) incidents in accordance with the school behaviour policy where appropriate.
- The school will inform parents/carers of any incidents of concerns as and when required.
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes as required.
- Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact the Integrated Front Door (019 or Warwickshire Police via 999 if there is immediate danger or risk of harm.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to Warwickshire Police.
- If the school is unsure how to proceed with any incidents of concern, then the incident will be escalated to the Education Safeguarding Team who may then be required to communicate wider issues to other schools/settings in Warwickshire.
- Parents and children will need to work in partnership with the school to resolve issues.

## **6. CYBER-BULLYING**

### **6.1 Definition**

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school Behaviour Policy).

### **6.2 Preventing and addressing cyber-bullying**

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

- The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.
- All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).
- The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.
- In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.
- The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

### 6.3 Examining electronic devices

- The headteacher, and any member of staff authorised to do so by the headteacher, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:
- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence.

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Assess how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from Headteacher.
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it.
- Seek the pupil's co-operation.

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so. When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the headteacher to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

They reasonably suspect that its continued existence is likely to cause harm to any person, and/or the pupil and/or the parent refuses to delete the material themselves.

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image.
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people.

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on [searching, screening and confiscation](#)
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people.
- Our Behaviour Policy.



Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

## **7. MANAGING INFORMATION SYSTEMS**

### **7.1 How will information systems security be maintained?**

- The security of the school information systems and users will be reviewed regularly.
- Virus protection will be updated regularly.
- Unapproved software will not be allowed in work areas or attached to email.
- Files held on the school's network will be regularly checked.
- The IT Technician will review system capacity regularly.
- The use of user logins and passwords to access the school network will be enforced.

### **7.2 How will the school website be managed?**

- The school will ensure that information posted on the school website meets the requirements as identified by the Department for Education.
- The contact details on the website will be the school address, email and telephone number. Staff or pupils' personal information will not be published.
- The Headteacher will take overall editorial responsibility for online content published by the school and will ensure that content published is accurate and appropriate.
- The school website will comply with the school's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.
- Pupils' images will only be published with the permission of their parents/carers and they will not be identified by name at any point.
- Only a small number of people will be given administration rights and all user accounts for the school website will be safeguarded with appropriately strong passwords.
- The school will post information about safeguarding, including online safety on the school website.

### **7.3 How will the use of images and videos be managed?**

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

### **7.4 How will email be managed?**

- Only staff and governors will be given access to school emails and will access these via their official school provided email accounts.
- Any electronic communication which contains any content which could be subject to data protection legislation must only be sent using secure and encrypted methods school email system).
- Members of the school community must immediately tell a designated member of staff if they receive offensive communication and this will be recorded in the school online safety incident log.
- Sensitive or personal information will only be shared via email in accordance with data protection legislation.

**Under no circumstances will staff communicate socially with pupils, whether past or present, via email and doing so will be seen as a disciplinary matter and may lead to dismissal.**

### **7.5 How will filtering be managed?**

The school's internet access strategy will be dependent on the need and requirements of our community and will therefore be designed to suit the age and curriculum requirements of our pupils, with advice from technical, educational and safeguarding staff.

The school uses educational filtered secure broadband connectivity through the WCC IT department which is appropriate to the age and requirement of our pupils.

The school uses the Smoothwall filtering system which blocks sites that fall into categories such as pornography, racial hatred, extremism, gaming, sites of an illegal nature, etc.

- The school's broadband access will include filtering appropriate to the age and maturity of pupils to try and prevent staff and pupils from being accidentally or deliberately exposed to unsuitable content.
- Inappropriate use of the internet, and breaches that may have safeguarding implications, are reported to the school directly through the local authority's monitoring and Smoothwall systems.
- There is a monthly online-safety report sent from WCC for the Headteacher to monitor usage which also flags up any concerns through their filtering.
- The school will work with WCC and the Schools Broadband team or broadband/filtering provider to ensure that filtering policy is continually reviewed.
- The school will have a clear procedure for reporting breaches of filtering which all members of the school community (all staff and all pupils) will be made aware of.
- If staff or pupils discover unsuitable sites, the URL will be reported to the School Designated Safeguarding Lead and will then be recorded and escalated as appropriate.
- Changes to the school filtering policy will be risk assessed by staff with educational and technical experience prior to any changes and where appropriate with consent from the Leadership Team.
- Any material that the school believes is illegal will be reported to appropriate agencies such as WSCB, Warwickshire Police or CEOP immediately.
- The Leadership Team will utilise the monthly digital monitoring report sent by WCC ICT department to ensure that the filtering methods selected are effective and appropriate.

### **7.6 How are emerging technologies managed?**

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Under normal circumstances there should be no reason why pupils will be using new and emerging technologies which have not been fully risk assessed and approved by the SLT with input from the Computing Learning Leader and WCC's ICT team.

### **7.7 How will apps used to record children's progress be managed?**

The Headteacher is ultimately responsible for the security of any data or images held of children. Apps/systems which store personal data will be risk assessed prior to use.

Personal staff mobile phones or devices will not be used for any apps which record and store children's personal details, attainment or photographs. The use of a mobile phone for photographs will only be undertaken in an emergency (e.g. to gather photographic evidence at the site of an accident), or by express permission of the SLT. This will only be done when photographs are for publication through

approved channels). All photographs will be immediately removed once shared via either the school website or to the main school account.

Only school-issued devices will be used for apps that record and store children's personal details or attainment.

Devices will be appropriately encrypted if taken off site to prevent a data security breach in the event of loss or theft.

Staff will be advised on safety measures to protect all members of the community such as using strong passwords, logging out of systems etc.

## **8. USE OF MOBILE PHONES AND PERSONAL DEVICES**

### **8.1 How will mobile phones and personal devices be managed?**

The use of mobile phones and other personal devices by pupils and staff in school is decided by the school and is covered in our Acceptable Use Policy. Staff may bring mobile phones into school but they must be switched off/muted and stored securely during lesson times and when a member of staff is directly in charge of children. Under no circumstances should a member of staff leave their mobile phone accessible to children.

If there are extenuating circumstances when a member of staff needs to have access to their mobile phone (such as a medical emergency), permission and agreement must first be sought from the Headteacher or other member of the SLT.

The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the school community and any breaches will be dealt with as part of the school Behaviour Policy.

School staff may confiscate a phone or device if they believe it is being used to contravene the schools' Behaviour or Anti-bullying Policy. If there is suspicion that the material on the mobile may provide evidence relating to a criminal offence the phone will be handed over to the police for further investigation.

Electronic devices of all kinds that are brought in to school are the responsibility of the user. The school accepts no responsibility for the loss, theft or damage of such items. Nor will the school accept responsibility for any adverse health effects caused by any such devices either potential or actual.

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

Should staff have a particular need to be available during school hours, they must obtain permission to have their mobile phone to hand from the Headteacher. In all but the most unusual of circumstances, the arrangement will be for the phone to be left on in the school office and taken directly to the member of staff when it rings or a message is sent.

### **8.2 Pupils Use of Personal Devices**

When a parent feels it is necessary for their child to bring a mobile phone to school (e.g. pupils in Year 6, who are walking to and from school and are permitted to bring mobile phones into school) the device should be switched off and handed into the office on arrival and can be collected when leaving the school premises at the end of the day. Under no circumstances should children have access to

their phone during the school day and devices are not to be left in pupils' bags or coats. Where this policy is not followed, the device will be confiscated and parents informed and requested to come into school to collect the item.

Digital watches – Digital watches that only work as a step counter are permitted – we know these can encourage children to be active. However, if a step counting watch also has the ability to be used for photos and communication, we will ask children not to wear these or to hand them in to the office on arrival each day. No Apple Watch devices are permitted for pupils.

Pupils should never use a personal device in a way that breaches the school's Behaviour or Anti-bullying Policies. If they do, the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents/carers at the Headteacher's discretion.

If a pupil needs to contact his/her parents/carers, a decision to do so will be made by the office and a message will be relayed on their behalf. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.

As part of curriculum learning in Upper Key Stage 2, pupils will be taught the importance of protecting their phone numbers by only giving them to trusted friends and family members. They will be instructed in safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences.

### **8.3 Staff Use of Personal Devices**

Staff are absolutely prohibited from using their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity.

Mobile Phone and devices will be switched off or switched to 'silent' mode, Bluetooth communication should be "hidden" or switched off and mobile phones or devices will not be used during teaching periods unless permission has been given by a member of SLT in emergency.

Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use work-provided equipment for this purpose (see above for details).

If a member of staff breaches the school policy then disciplinary action will be taken.

### **8.4 Visitors' use of Personal Devices**

Parents/carers and visitors must use mobile phones and personal devices in accordance with the school's policy, although they will not be expected to leave them in the school office.

Use of mobile phones or personal devices by visitors and parents/carers to take photos or videos must take place in accordance with the School Image Use Policy.

Staff will be expected to challenge concerns when safe and appropriate and will always inform the Designated Safeguarding Lead of any breaches of use by visitors.

## **9. HOW THE SCHOOL WILL RESPOND TO ISSUES OF MISUSE**

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on Behaviour Policy and Acceptable Use Agreement. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the Staff Disciplinary Procedures and Staff Code of Conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

## **10. TRAINING**

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse.
- Children can abuse their peers online through:
  - Abusive, harassing, and misogynistic messages.
  - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups.
  - Sharing of abusive images and pornography, to those who don't want to receive such content.
  - Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element.

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse.
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks.
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term.

The DSL deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our Child Protection and Safeguarding Policy.

## **11. MONITORING ARRANGEMENTS**

The DSL and staff log behaviour and safeguarding issues related to online safety.

This policy will be reviewed every year. At every review, the policy will be shared with the governing board. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

## **12. LINKS WITH OTHER POLICIES**

This online safety policy is linked to our:

Child protection and Safeguarding Policy  
Behaviour policy  
Staff Behaviour Policy  
Staff Disciplinary Procedures  
Data Protection Policy and Privacy Notices  
Complaints Procedure  
Internet Acceptable Use Policy and Agreements