



## St Leonard's CE(A) First School Policy for Online Safety



*'Let your light shine before others so that they may see your good works and give glory to your Father who is in heaven.'*

*Matthew 5:16*

Adopted by the Governing Board:

May 2023

Date for review: May 2024

Date of last policy reviewed	Changes made
May 2017	Filtering system changed to Futures Cloud from PCE. GDPR Requirements.
May 2018	Dates changed
May 2019	Dates changed Computing lead added as checking the computer filtering systems alongside the Headteacher.
May 2020	Dates and Miss Torr as Computing lead changed.
May 2022	Complete revision of policy taking into account: KCSIE 2021 update The Key for school leadership model policy Guidance from the National Cyber Security Centre and the UK Council for Internet Safety, DFE Teaching Online Safety in school
May 2023	Additions to section 3 - Governing Board to ensure that online safety is a running theme.  Addition to section 5 - 'The school will let the parents know what systems the school uses for filtering and monitoring online use. They will tell parents what their children are being asked to do online.'  Additions to section 6.3 - Searching and confiscation of electronic devices in line with KCSIE.

## St. Leonard's CE (A) First School



### Online Safety Policy

#### Contents

<a href="#">1. Aims</a> .....	3
<a href="#">2. Legislation and guidance</a> .....	4

<a href="#">3. Roles and responsibilities</a> .....	4
<a href="#">4. Educating pupils about online safety</a> .....	7
<a href="#">5. Educating parents about online safety</a> .....	9
<a href="#">6. Cyber-bullying</a> .....	9
<a href="#">7. Acceptable use of the internet in school</a> .....	11
<a href="#">8. Pupils using mobile devices in school</a> .....	11
<a href="#">9. Cyber-Security</a> .....	11
<a href="#">10. Social Media</a> .....	13
<a href="#">11. How the school will respond to issues of mis-use</a> .....	23
<a href="#">12. Prevent Duty</a> .....	24
<a href="#">13. Training</a> .....	24
<a href="#">14. Monitoring Arrangements</a> .....	
<a href="#">15. Links with other policies</a> .....	
<a href="#">Appendix 1: EYFS acceptable use agreement (pupils and parents/carers)</a> .....	25
<a href="#">Appendix 2: KS1 acceptable use agreement (pupils and parents/carers)</a> .....	
<a href="#">Appendix 3: KS2 acceptable use agreement (pupils and parents/carers)</a> .....	
<a href="#">Appendix 4: acceptable use agreement (staff, governors, volunteers and visitors)</a> .....	26
<a href="#">Appendix 5: online safety training needs – self audit for staff</a> .....	28
<a href="#">Appendix 6: online safety incident report log</a> .....	<b>Error! Bookmark not defined.</b>

---

## 1. Aims

Our school aims to:

- Value the internet as an essential element in 21<sup>st</sup> Century life for Education, business and social interaction offering unimaginable opportunities.
- Stay current with rapidly evolving technology in order to educate our pupils.
- Provide pupils with quality internet access to enhance their learning experience as part of the statutory curriculum.
- Educate pupils in the effective use of the internet in research.
- Teach pupils how to evaluate internet content, be critically aware of materials they read validating information before accepting its validity.
- 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.

### 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, anti-Semitism, 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 purpose
- **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; and
- **Commerce** - risks such as online gambling, inappropriate advertising, phishing and/or financial scam

## 2. Legislation and guidance

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

[Teaching online safety in schools](#)

[Preventing and tackling bullying](#) and [cyber-bullying: advice for headteachers and school staff](#)

[\[Relationships and sex education](#)

[Searching, screening and confiscation](#)

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 takes into account 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 ensure that online safety is a running and interrelated theme whilst devising and implementing their whole school approach to safeguarding and related policies and procedures.

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 Governing Board make use of guidance from the UK Council for Internet Safety to support and challenge online safety provision.

The governor who oversees online safety is Mrs Jackie Worrall.

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 (appendix 3)
- Ensure that children's exposure to online safety risks is minimized with appropriate filtering and monitoring systems informed by the school's Prevent Risk Assessment.
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with SEND 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 DSL and deputies are set out in our child protection and safeguarding policy as well as relevant job descriptions.

The DSL is also the Headteacher and 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 staff, as necessary, to address any online safety issues or incidents.
- Maintaining a current record of all staff and pupils who are granted access to school ICT systems.
- Ensures that the school website does not contain staff or pupil's personal information and that written permission is gained from parents before publishing photographs of children on the website.
- Managing all online safety issues and incidents in line with the school child protection policy
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy.
- Providing regular reports on online safety in school to the governing board.
- Ensuring that any online safety incidents are logged (see appendix 5) 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

### 3.3 The Online Safety Lead

- Updating and delivering staff training on online safety (appendix 4 contains a self-audit for staff on online safety training needs)

- Liaising with other agencies and/or external services if necessary
- Arranging external visitors to deliver online safety education if appropriate. The guidance on *Using external visitors to support online safety education* from UKCCIS will be used to ensure this process is effective.

### 3.4 The ICT technician in conjunction with the DSL

The ICT technician is 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. St Leonards uses the Futures Cloud system.

*The school will take all reasonable precautions to prevent access to inappropriate material. It is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed or consequences of internet access.*

- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly to tackle evolving cyber-crime technologies.
- Conducting a full security check and monitoring the school's ICT systems on a monthly basis or as and when an incident occurs.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.

### 3.5 All staff and volunteers

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 (appendix 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2).
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 5) 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.
- 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'.

### 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 (appendices 1 and 2)

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](#)

Parent resource sheet - [Childnet International](#)

Healthy relationships - [Disrespect Nobody](#)

St Leonards aims to work alongside parents in a continuing learning journey around their children's use of technology and the challenges and dangers they face. Parents are kept informed through our weekly newsletter and we provide parent workshops to explore online safety in more detail.

### 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 before being granted access to school ICT systems. (appendix 3).

## 4. Educating pupils about online safety

### 4.1 Digital resilience

At St Leonard's we aim to nurture 'digital resilience' in our pupils. This develops as they spend time online and face the challenges out there. Being able to explore with set boundaries. We want them to recognise when they are at risk online and that they know what to do when that happens. A resilient child is more likely to stay safe if anything bad happens, and benefit from the opportunities the online world provides. It is important that our pupils understand how to report online material that makes them feel unsafe.

### 4.2 Digital Life Skills

At St Leonard's we place the same importance on digital life skills as other life skills such as crossing the road and swimming.

- **A Critical Thinker**

Spotting misinformation or lies

Knowing when a website is giving advice that is wrong or potentially harmful.

Recognising and rejecting peer pressure to join in with online crazes that could hurt them or someone they know.

- **A Confident Communicator**

Confidence to ask for help when they need someone to talk to or things go wrong or upset them.

Ask for help even when they've done something they shouldn't have

- **A Capable Tools User**



Using tools to make their internet use safe and positive. Tools such as unique passwords and anti-virus software to keep their information private.

How to block people on apps and services.

How to adjust safety and privacy settings.

How to check their digital footprint and keep it positive.

Use the internet to allow their creativity to flourish.

### 4.3 Digital well-being

A section of our PSHCE and RSHE Curriculum is judging the impact of online activity on quality of life, physical and mental health and relationships. Supporting pupils to recognise their use of screen time and managing this by gaining a balance.

Screen time varies enormously by the context in which it is used. Our role is to open children up to the possibilities of technology and how they can use it creatively and positively and recognise that it should be an addition to our lives and should not replace eating and sleeping well, being physically healthy, connecting socially, engaging in learning and enjoying and pursuing hobbies and interests.

### 4.4 Online safety in the curriculum

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

All schools have to teach:

[Relationships education and health education](#) in primary schools

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:

- 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: (some of this content will be taught in Years 5 and 6 when our pupils transition to Middle School.

- 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.

### **Computing Curriculum**

The above curriculum complements that of the Computing curriculum, which covers the principles of online safety at all key stages with progression in the content to reflect the different and escalating risks that pupils face.

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

### **4.5 Bespoke Online Safety Education**

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

Teaching staff explore the sites and apps that our pupils use. We encourage an open discussion about this so that we can tailor our curriculum to their direct needs.

## **5. Educating parents about online safety**

The school will raise parents' awareness of internet safety in weekly newsletters or other communications home, and in information via our website or seesaw learning platform. This policy will also be shared with parents.

The school will let the parents know what systems the school uses for filtering and monitoring online use. They will tell parents what their children are being asked to do online.

Online safety will also be covered during parent consultations and parent workshops.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher/ DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

## **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. Our Christian ethos fosters a culture of kindness, of respect and love supporting our pupils to be a buddy not a bully. We teach our pupils to have courage to report when they know something is not right. They are taught that their behaviour on line should be as good as their behaviour in person.

There are planned opportunities for teaching staff to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHCE) and (RSHE) 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 via its weekly newsletter 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 consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

### 6.3 Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

Only authorised staff (The Headteacher/ DSL or deputy DSL's) may search and confiscate electronic devices. They MUST be satisfied that they have reasonable grounds for suspecting that a pupil is in possession of an electronic device that poses a risk before taking steps to search.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If the search is not urgent the member of staff should seek advice from the Headteacher or DSL.

If a member of staff believes a device may contain a nude or semi-nude image or an image it is criminal to possess, they will not view the image but will report it to the DSL. The DSL will decide what to do next in line with the relevant guidance.

If inappropriate material is found on the device, the DSL or other member of the senior leadership team will decide whether they should:

- Delete that material, or

- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police\*

\* Authorised staff may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse includes an online element.

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

- The DfE's latest guidance on [screening, searching and confiscation](#)
- UKCIS guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#)
- The school's COVID-19 risk assessment

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. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1-3). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

These agreements will be displayed in classrooms and the staffroom.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above. All will be made aware that internet traffic can be monitored and traced to an individual user.

More information is set out in the acceptable use agreements in appendices 1, 2 and 3.

## 8. Pupils using mobile devices in school

The use of mobile devices is not allowed at St Leonard's school due to the age of our pupils.

## 9. Cyber-Security

### 9.1 The aim of Cyber-Security

Cyber-Security is 'protecting the devices we use and services we access online both at home and at work from theft'. Preventing un-authorized access to the vast amount of personal information we store on these devices and online.

Staff should work within a culture of 'questioning' and if something looks strange should get a second opinion.

### 9.2 Staff using work devices inside and outside of school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected - strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted - this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device

- Using USB devices with care.
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date - always install the latest updates
- Watching out for fake emails.

Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 3.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the DSL, Online safety Lead or the ICT Technician.

## 10. Social Media - Protecting Professional Identity

All schools have a duty of care to provide a safe learning environment for pupils and staff.

Schools could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions.
- Risk assessment, including legal risk.

School staff should ensure that:

- No reference should be made in social media to students / 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 or local authority.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

The school's use of social media for professional purposes will be checked regularly by the Headteacher to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies.

The use of social networking and on-line media

This school asks its whole community to promote the 3 commons approach to online behaviour:

- Common courtesy
- Common decency
- Common sense

How do we show common courtesy online?

- We ask someone's permission before uploading photographs, videos or any other information about them online.
- We do not write or upload 'off-hand', hurtful, rude or derogatory comments and materials. To do so is disrespectful and may upset, distress, bully or harass.

**How do we show common decency online?**

- We do not post comments that can be considered as being intimidating, racist, sexist, homophobic or defamatory. This is cyber-bullying and may be harassment or libel.
- When such comments exist online, we do not forward such emails, tweets, videos, etc. By creating or forwarding such materials we are all liable under the law.

**How do we show common sense online?**

- We think before we click.
- We think before we upload comments, photographs and videos.
- We think before we download or forward any materials.
- We think carefully about what information we share with others online, and we check where it is saved and check our privacy settings.
- We make sure we understand changes in use of any web sites we use.
- We block harassing communications and report any abuse.

Any actions online that impact on the school and can potentially lower the school's (or someone in the school) reputation in some way or are deemed as being inappropriate will be responded to.

In the event that any member of staff, student or parent/carer is found to be posting libellous or inflammatory comments on Facebook or other social network sites, they will be reported to the appropriate 'report abuse' section of the network site.

(All social network sites have clear rules about the content which can be posted on the site and they provide robust mechanisms to report contact or activity which breaches this.)

## **11. 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 below. 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 behaviour policy/ code of conduct. The action

taken will depend on the individual circumstances, nature and seriousness of the specific incident as detailed below.

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

### Appropriate use of ICT by Staff and pupils

	Staff & other adults			Students / Pupils				
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
<b>Communication Technologies</b>								
Mobile phones may be brought to school	✓			✓				
Use of mobile phones in lessons				✓				
Use of mobile phones in social time	✓			✓				
Taking photos on mobile phones / cameras		✓		✓				
Use of other mobile devices eg tablets, gaming devices							✓	
Use of personal email addresses in school, or on school network			✓	✓				
Use of school email for personal emails				✓				
Use of messaging apps				✓				

Use of social media			✓	✓				
Use of blogs	✓				✓			

**Unsuitable / inappropriate activities**

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts usage as follows:

**User Actions**

		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images -The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	criminally racist material in UK - to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	pornography				X	
	promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	



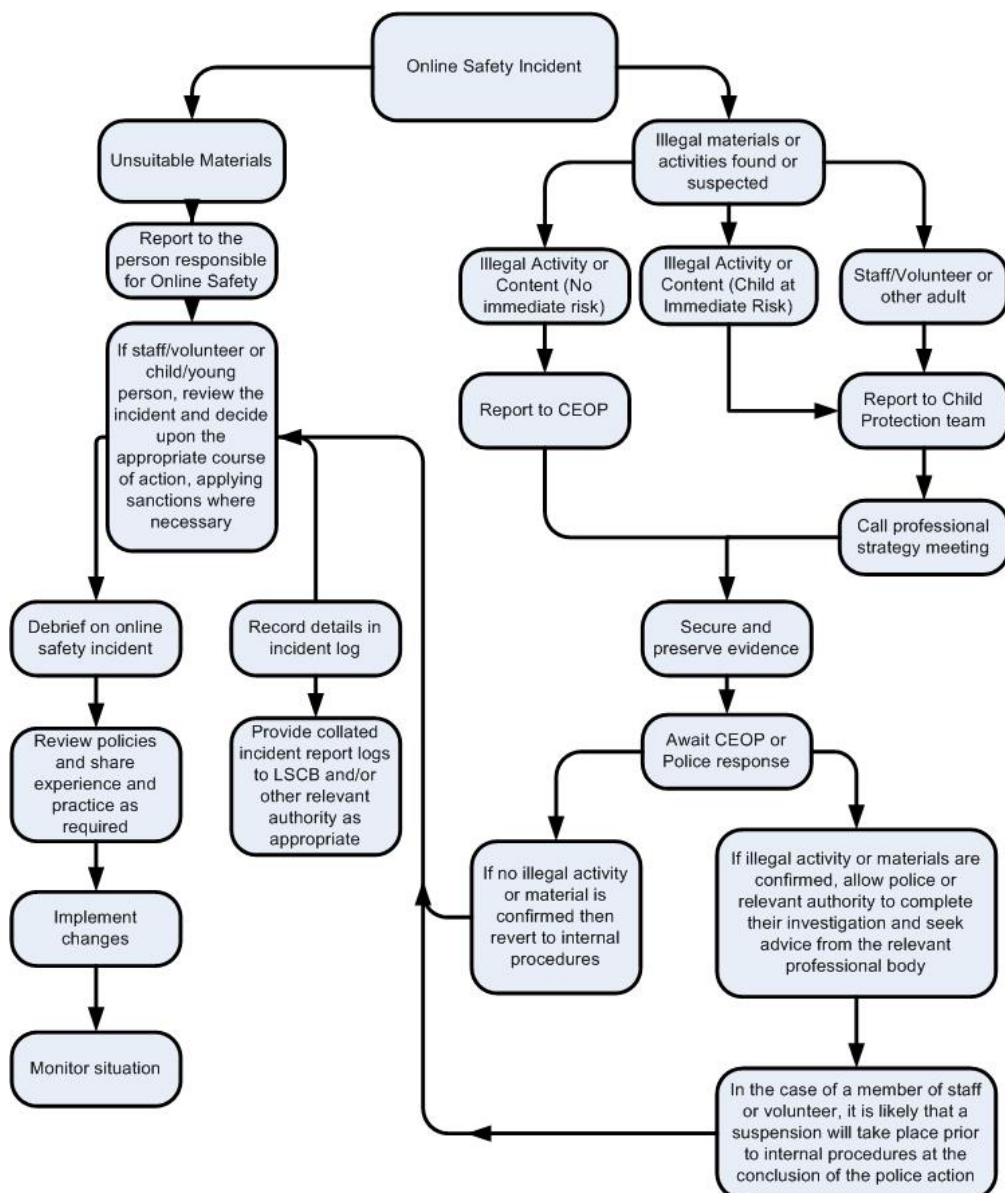
Using school systems to run a private business				X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school				X	
Infringing copyright				X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)				X	
Creating or propagating computer viruses or other harmful files				X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)				X	
On-line gaming (educational)				X	
On-line gaming (non educational)				X	
On-line gambling				X	
On-line shopping / commerce			X		
File sharing			X		
Use of social media			X		
Use of messaging apps				X	
Use of video broadcasting eg Youtube		X			

### Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see "User Actions" above).

### Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.



### Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

### Procedures

#### General

All incidents should be dealt with on an individual case by case basis, and an escalating tariff of agreed sanctions put in place.

The context, intention and impact of each incident should determine the response and actions to be taken. This allows a degree of flexibility in the application of sanctions. For example, a series of minor incidents by one individual is likely to be treated differently than a one-off occurrence; similarly unintentional and intentional access to inappropriate websites will instigate different levels of intervention and sanctions.

All online safety incidents should be recorded and monitored, and any potential patterns in behaviours identified, to enable such issues to be addressed proactively and for protection to be afforded.

## **All incidents**

The following procedure should be followed for all incidents.

- The incident should be reported to the senior designated person for safeguarding. A written incident record should be made, and the situation monitored.
- The context, intention and impact of such misuse must also be considered. Where deemed necessary the incident may be escalated to a 'serious' level.
- If the incident relates to the inadvertent access to an inappropriate website, it should be added to the banned or restricted list and filters should be applied, where relevant.
- In respect of misuse by children and young people, parents and carers must be informed of the alleged incident and should be advised of any actions to be taken as a result.
- Sanctions should be applied in accordance with the acceptable use policy.

There will always be the possibility that through access to the internet children and young people may gain unintentional access to inappropriate materials. Such material may not be illegal, but is unsuitable in a childcare environment and should be acted on.

## **Reporting**

An open reporting policy should be in place which means that all inadvertent breaches and access to inappropriate materials are reported. The non-reporting of such breaches should result in the concern being escalated.

## **Serious Incidents**

All serious incidents must be dealt with promptly and reported to the senior designated person for safeguarding and the registered person immediately. The context, intention and impact of the alleged misuse must be considered.

Appropriate actions should be agreed between the senior designated person for safeguarding and the registered person. All details should be accurately and legibly recorded. The reason why any decision is made should also be noted.

If at any stage a child or young person is or has been subject to abuse of any form, the safeguarding policy should be implemented with immediate effect. A referral should be made through Staffordshire County Council protection procedures or through children's social care and the police, where applicable.

If the incident relates to an allegation made against an employee, manager, volunteer or student; and there is a suggestion that a child or young person has been subject to any form of abuse, the safeguarding policy will again be implemented with immediate effect. The local authority designated officer must be contacted in the first instance in respect of any allegation made against an adult. The police and Ofsted must also be contacted.

No internal investigation or interviews should be carried out in respect of any allegations, unless explicitly requested otherwise by an investigating agency.

If allegations of abuse are made, children's social care, the police and/or the Local Authority designated officer will be the investigative bodies. It must therefore be ensured that no action is taken which could compromise any such investigations.

Where applicable, any hardware implicated in any potential investigations of misuse should be secured, so that evidence can be preserved. This may include mobile phones, laptops, computers and portable media technology.

Internal disciplinary procedures should not be undertaken until investigations by the relevant agencies have been completed. Legal or human resources advice should be sought prior to carrying out any internal investigations and/or instigating high-level disciplinary procedures.

On completion of both internal and external investigations, or sooner where appropriate, an online safety review should be undertaken and policies and procedures amended and updated as necessary. A consultation on any proposed revisions should be held with all ICT users as appropriate. Revised policies and procedures should be circulated as applicable.

By nature, serious incidents most often involve illegal materials and activities, including the viewing, possession, taking, making and distribution of indecent images; bullying or harassment through the use of 30 portable media devices such as mobile phones, or grooming. These incidents may be instigated by a child, young person or adult.

The following incidents must always be reported to the police, SSCB, children's social care, Local authority designated officer and Ofsted.

- Discovery of indecent images of children and young people.
- Behaviour considered to be 'grooming'.
- Sending of obscene materials. By not reporting such incidents, an offence may be committed.

The seriousness of such allegations should be fully recognised, and all such incidents must be reported to the police immediately. No attempt should be made to download, print or send any materials found. Further offences could be committed by doing so.

If potentially illegal material is discovered, as far as is reasonable practical, the equipment or materials found should not be touched. Computers or other devices should not be switched off unless authorised to do so by the police. The focus must be on preventing further access to the illegal content by keeping other individuals out of the immediate area. Where necessary the monitor should be turned off (but the computer remains on).

#### **Illegal material and activities which must be reported to the Internet Watch Foundation**

A report should also be made to the Internet Watch Foundation - <http://www.iwf.org.uk/reporting.htm>

If potentially illegal materials, including images of child abuse have been accessed online, giving details of the website address. If it is unclear whether the content is illegal or not, the concern should be reported as a matter of caution.

#### **Media attention**

If a serious incident occurs, it may attract intense media interest and speculation. On such occasions, every possible attempt should be made to ensure that children and young people, parents and carers are protected and supported appropriately.

An agreed media strategy should be implemented, and statements only released by authorised personnel, in accordance with information sharing procedures. In all instances, the prime concern should be the safeguarding and welfare of the children, young people and their families. Advice should be taken from services for children and young people where appropriate before any media engagement is undertaken.

#### **In the event of suspicion, all steps in this procedure should be followed:**

- Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.

- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse - see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
  - Internal response or discipline procedures
  - Involvement by Local Authority or national / local organisation (as relevant).
  - Police involvement and/or action

If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:

- incidents of 'grooming' behaviour
- the sending of obscene materials to a child
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

### **School Actions & Sanctions**

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:

#### **Students / Pupils**

---

Incidents:	Refer to class teacher	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents and carers	Removal of network / internet access rights	Warning	Further sanction
<b>Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).</b>		X	X					
Unauthorised use of non-educational sites during lessons	X						X	
Unauthorised use of mobile phone / digital camera / other mobile device	X	X			X			
Unauthorised use of social media / messaging apps / personal email					X		X	
Unauthorised downloading or uploading of files	X			X				
Allowing others to access school network by sharing username and passwords	X						X	
Attempting to access or accessing the school network, using another student's / pupil's account	X						X	
Attempting to access or accessing the school network, using the account of a member of staff		X			X			X
Corrupting or destroying the data of other users				X				X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X	X		X			X
Continued infringements of the above, following previous warnings or sanctions		X		X				X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X		X				X
Using proxy sites or other means to subvert the school's / academy's filtering system					X		X	
Accidentally accessing offensive or pornographic material and failing to report the incident		X	X	X	X		X	X
Deliberately accessing or trying to access offensive or pornographic material		X	X		X			X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act		X						X

**Staff**

**Actions / Sanctions**

Incidents:	Refer to line manager	Refer to Headteacher	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
<b>Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).</b>	X	X		X				X
Inappropriate personal use of the internet / social media / personal email	X	X				X		
Unauthorised downloading or uploading of files	X				X	X		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	X				X	X		
Careless use of personal data eg holding or transferring data in an insecure manner	X					X		
Deliberate actions to breach data protection or network security rules		X			X	X		X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X			X	X		X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X	X	X			X	X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils		X	X					X
Actions which could compromise the staff member's professional standing		X	X					X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X					X	
Using proxy sites or other means to subvert the school's filtering system	X					X	X	
Accidentally accessing offensive or pornographic material and failing to report the incident		X	X					
Deliberately accessing or trying to access offensive or pornographic material				X			X	
Breaching copyright or licensing regulations		X						X
Continued infringements of the above, following previous warnings or sanctions		X					X	X

## 12. PREVENT Duty



In accordance with the Prevent Strategy, which aims to prevent children and young people being exposed to extremist views and at risk of radicalisation, staff are all trained on the channel programme [http://course.ncalt.com/Channel\\_General\\_Awareness/01/index.html](http://course.ncalt.com/Channel_General_Awareness/01/index.html)

This responsibility extends to online safety and protecting children from extremist material online.

Through this training, staff are aware of how the internet is used to radicalise people. Filtering should prevent access to such extremist sites but any material accessed at school should be treated as an online safety incident and dealt with accordingly.

Disclosures or concerns regarding exposure outside of school should be treated as a safeguarding incident and dealt with in accordance with the Safeguarding policy and procedures (cf. Safeguarding policy).

Parents and carers are informed about the risks of radicalisation and extremism via online safety newsletters and The Prevent Action Plan which is available the school website.

### 13. 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 the risks up
- 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 and 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.

## 14. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 5.

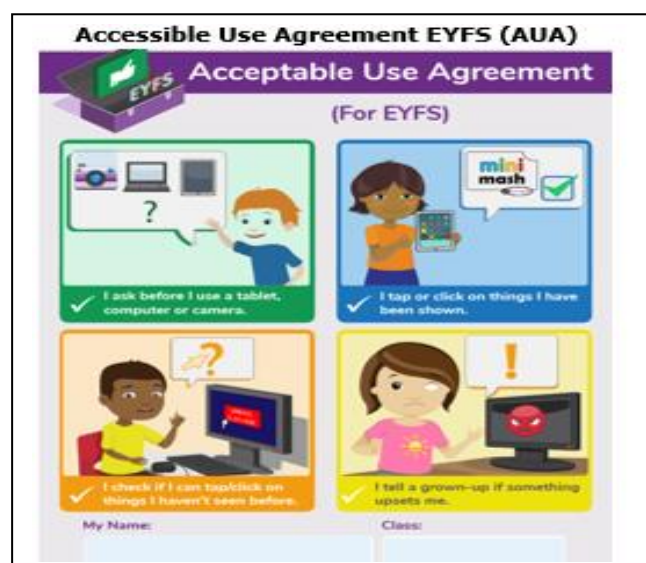
This policy will be reviewed every year by the DSL and Online Safety Lead. At every review, the policy will be shared with the governing board. The review be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

## 15. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Staff Behaviour Policy (Code of Conduct)
- Data protection policy and privacy notices
- Complaints procedure
- Anti-bullying Policy
- ICT and internet acceptable use policy
- Mobile phone and digital communications Policy

## Appendix 1: EYFS acceptable use agreement (pupils and parents/carers)



## Appendix 2: KS1 acceptable use agreement (pupils and parents/carers)

### ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS

Name of pupil:

**When I use the school's ICT systems (like computers and I-pads) and get onto the internet in school I will:**

Ask a teacher or adult if I can do so before using them

Only use websites that a teacher or adult has told me or allowed me to use

Tell my teacher immediately if:

- I click on a website by mistake
- I receive messages from people I don't know
- I find anything that may upset or harm me or my friends

Use school computers and I-pads for school work only

Be kind to others and not upset or be rude to them

Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly

Only use the username and password I have been given

Try my hardest to remember my username and password

Never share my password with anyone, including my friends.

Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer

Save my work on the school network

Check with my teacher before I print anything

Log off or shut down a computer/ I-pad when I have finished using it

**I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.**

**Signed (pupil):**

**Date:**

**Parent/carer agreement:** I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and will make sure my child understands these.

**Signed (parent/carer):**

**Date:**

## Appendix 3: KS2 acceptable use agreement (pupils and parents/carers)

### ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS

Name of pupil:

**I will read and follow the rules in the acceptable use agreement policy**

**When I use the school's ICT systems (like computers/ I-pads) and get onto the internet in school I will:**

Always use the school's ICT systems and the internet responsibly and for educational purposes only

Only use them when a teacher is present, or with a teacher's permission

Keep my username and passwords safe and not share these with others

Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer

Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others

Always log off or shut down a computer when I'm finished working on it

**I will not:**

Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity

Open any attachments in emails, or follow any links in emails, without first checking with a teacher

Log in to the school's network using someone else's details

Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision

**I will not bring a personal mobile phone or other personal electronic device into school.**

**I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.**

**Signed (pupil):**

**Date:**

**Parent/carer agreement:** I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and will make sure my child understands these.

**Signed (parent/carer):**

**Date:**

## Appendix 4: acceptable use agreement (staff, governors, volunteers and visitors)

### ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS



**Name of staff member/governor/volunteer/visitor:**

**When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not:**

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Use them in any way which could harm the school's reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the school's network
- Share my password with others or log in to the school's network using someone else's details
- Take photographs of pupils without checking with teachers first
- Share confidential information about the school, its pupils or staff, or other members of the community
- Access, modify or share data I'm not authorised to access, modify or share
- Promote private businesses, unless that business is directly related to the school
- Download apps from non-official stores.

I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.

I will only use my school email address for school business.

I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.

I will take all reasonable steps to ensure that work devices are secure (e.g locking my device when I'm not using it) and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.


I will let the designated safeguarding lead (DSL) and ICT technician know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.


**Signed (staff member/governor/volunteer/visitor):**

**Date:**

## Appendix 5: online safety training needs – self audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT 	
<b>Name of staff member/volunteer:</b>	<b>Date:</b>
Question	Yes/No (add comments if necessary)
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways pupils can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

## Appendix 6: online safety Incident Log

	Online safety Incident Log
---	----------------------------

Online safety Lead Teacher		
Online safety Lead Governor		
Details of Online safety Incident		
Type of incident	Bullying or harassment	
	Online bullying or harassment	
	Sexting (self-taken indecent images)	
	Deliberately bypassing security or access	
	Hacking or virus propagation	
	Racist, sexist, homophobic, religious hate material	
	Terrorist material	
	Sexual images/ pornography	
	Other (Please specify) .....	
Date of Incident		
Time of Incident		
Where the incident occurred		
Name of person reporting the incident		
Who was involved in the incident	Child/ young person	
	Staff member	
	Other (Please specify)	

Description of the incident		
Nature of the incident	Accidental	
	Deliberate	
Did the incident involve material being...	Created	
	Viewed	
	Printed	
	Shown to others	
	Transmitted to others	
	Distributed	
Could this incident be considered as...	Harassment	
	Grooming	
	Cyberbullying	
	Sexting (self taken indecent imagery)	
	Breach of acceptable use policy	
	Other (please specify) .....	
	Staff	
	Incident reported to head/ senior leader	
	Child involved (if necessary)	
	Parents informed	
	Disciplinary action taken (please specify)	



	Child debriefed	
	Senior leader/ Online safety Lead	
	Advice sought from children's social care	
	Incident reported to police	
	Incident reported to CEOP	
	Incident reported to Internet Watch Foundation	
	Incident reported to IT services	
	Online safety policy to be reviewed/ amended	

Outcome of incident/ investigation		
Children's Social Care		
Police/ CEOP		
School		
Individual staff member/ child		
Parents		
Other (HR/ Legal etc)		

Learning from the case		
Key Learning Point 1		
Key Learning Point 2		
Key Learning Point 3		

Recommendations and Timescales			
Recommendation 1		Timescale to be implemented	
Recommendation 2		Timescale to be implemented	
Recommendation 3		Timescale to be implemented	