

Online Safety Policy



Serenity School

Approved by:	Chief Operating Officer
Last reviewed on:	01/09/2026
Next review due by:	01/09/2027

Contents

This policy applies to all Serenity Schools. References to 'the school' mean the individual Serenity school in which the policy is being applied.	2
1. Aims	2
2. Legislation and guidance	3
3. Roles and responsibilities	3
4. Educating pupils about online safety	6
5. Educating parents/carers about online safety	8
6. Cyber-bullying	8
7. Acceptable use of the internet in school	9
8. Pupils using mobile devices in school	10
9. Staff using work devices outside school	10
10. How the school will respond to issues of misuse	10
11. Training for staff, proprietary board and volunteers	10
12. Monitoring arrangements	11
13. Links with other policies	11
Appendix 1: online safety training needs – self-audit for staff	13

This policy applies to all Serenity Schools. References to 'the school' mean the individual Serenity school in which the policy is being applied.

1. Aims

Our school aims to:

- › Have robust processes in place to ensure the online safety of pupils, staff, volunteers and proprietary board
- › Identify and support groups of pupils that are potentially at greater risk of harm online than others
- › 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, misinformation, disinformation (including fake news), conspiracy theories, 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 the user 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; and
- › **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](#)
- › [Meeting digital and technology standards](#)
- › [Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff](#)
- › [Relationships and sex education \(RSE\) and health 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.

3. Roles and responsibilities

3.1 The proprietary board

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

The proprietary board will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The proprietary board will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

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

The proprietary board will make sure that the school teaches pupils how to keep themselves and others safe, including online.

The proprietary board will make sure that the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the [DfE's filtering and monitoring standards](#), and discuss with IT staff and service providers what needs to be done to support the school in meeting the standards, which include:

- › Identifying and assigning roles and responsibilities to manage filtering and monitoring systems
- › Reviewing filtering and monitoring provisions at least annually
- › Blocking harmful and inappropriate content without unreasonably impacting teaching and learning
- › Having effective monitoring strategies in place that meet the school's safeguarding needs

The Chair of the Proprietary Board is responsible for overseeing and scrutinising the school's annual filtering and monitoring review and providing assurance to the proprietary board that the required standards are being met.

The proprietary board will:

- › Make sure 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
- › Make sure that online safety is a running and interrelated theme when devising and implementing the whole-school or college approach to safeguarding and related policies and/or procedures

- › Make sure 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 of each school is the senior leader responsible for ensuring that the filtering and monitoring standards are met within that school. Each school's annual review will be led by the headteacher and supported by the DSL, Group Safeguarding Lead and IT support. The Chair of the Proprietary Board will oversee and scrutinise the completed reviews and provide assurance to the proprietary board.

3.3 The designated safeguarding lead (DSL)

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:

- › Supporting the headteacher in making sure that staff understand this policy and that it is being implemented consistently throughout the school
- › Working with the headteacher to review this policy annually and make sure the procedures and implementation are updated and reviewed regularly
- › Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- › Providing the proprietary board with assurance that filtering and monitoring systems are working effectively and reviewed regularly
- › Working with the ICT manager to make sure the appropriate systems and processes are in place
- › 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's child protection policy
- › Responding to safeguarding concerns identified by filtering and monitoring
- › Making sure that any online safety incidents are logged and dealt with appropriately in line with this policy
- › Making sure that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- › Updating and delivering staff training on online safety (appendix 1 contains a self-audit for staff on online safety training needs)
- › Liaising with other agencies and/or external services if necessary
- › Providing regular reports on online safety in school to the headteacher and/or proprietary board
- › Undertaking annual risk assessments that consider and reflect the risks pupils face
- › Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

3.4 The ICT provider

The ICT provider is responsible for:

- › Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to

assess effectiveness and make sure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material

- › Making sure 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 regular basis
- › Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- › Making sure that any online safety incidents are logged and dealt with appropriately in line with this policy
- › Making sure that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- › Maintaining the filtering and monitoring systems, providing appropriate reports, participating in checks and the annual review, and completing technical actions arising from concerns, system failures or identified gaps.

This list is not intended to be exhaustive.

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, and making sure that pupils follow the school's terms on acceptable use
- › Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing
- › Following the correct procedures by Techlogic IT Services if they need to bypass the filtering and monitoring systems for educational purposes
- › Working with the DSL to make sure that any online safety incidents are logged and dealt with appropriately in line with this policy
- › Making sure 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/carers

Parents/carers are expected to:

- › Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- › Make sure that 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/carers can seek further guidance on keeping children safe online from the following organisations and websites:

- › What are the issues? – [UK Safer Internet Centre](#)
- › Help and advice for parents/carers – [Childnet](#)
- › Parents and carers resource sheet – [Childnet](#)

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 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

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

The primary and secondary expectations below will be applied according to pupils' age, developmental stage and individual needs. Where a school does not provide a particular phase of education, the relevant content is included to identify expected prior learning and areas that some pupils may need to revisit.

Primary

In **Key Stage (KS) 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 (KS) 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
- › Be discerning in evaluating digital content

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

- › That people should be respectful in online interactions, and that the same principles apply to online relationships as to face-to-face relationships, including where people are anonymous. For example, the importance of avoiding putting pressure on others to share information and images online, and strategies for resisting peer pressure
- › How to critically evaluate their online relationships and sources of information, including awareness of the risks associated with people they have never met. For example, that people sometimes behave differently online, including pretending to be someone else, or pretending to be a child, and that this can lead to dangerous situations. How to recognise harmful content or harmful contact, and how to report this
- › That there is a minimum age for joining social media sites (currently 13), which protects children from inappropriate content or unsafe contact with older social media users, who may be strangers, including other children and adults
- › The importance of exercising caution about sharing any information about themselves online. Understanding the importance of privacy and location settings to protect information online
- › Online risks, including that any material provided online might be circulated, and that once a picture or words has been circulated there is no way of deleting it everywhere and no control over where it ends up
- › That the internet contains a lot of content that can be inappropriate and upsetting for children, and where to go for advice and support when they feel worried or concerned about something they have seen or engaged with online

Secondary

In **KS3**, pupils will be taught to:

- › Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy

- › Recognise inappropriate content, contact and conduct, and know how to report concerns

Pupils in **KS4** will be taught:

- › To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- › How to report a range of concerns

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

- › Rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- › Online risks, including the importance of being cautious about sharing personal information online and of using privacy and location settings appropriately to protect information online. Pupils should also understand the difference between public and private online spaces and related safety issues
- › The characteristics of social media, including that some social media accounts are fake, and / or may post things which aren't real / have been created with AI. That social media users may say things in more extreme ways than they might in face-to-face situations, and that some users present highly exaggerated or idealised profiles of themselves online
- › Not to provide material to others that they would not want to be distributed further and not to pass on personal material which is sent to them. Pupils should understand that any material provided online might be circulated, and that once this has happened there is no way of controlling where it ends up. Pupils should understand the serious risks of sending material to others, including the law concerning the sharing of images
- › That keeping or forwarding indecent or sexual images of someone under 18 is a crime, even if the photo is of themselves or of someone who has consented, and even if the image was created by the child and/or using AI-generated imagery. Pupils should understand the potentially serious consequences of acquiring or generating indecent or sexual images of someone under 18, including the potential for criminal charges and severe penalties including imprisonment. Pupils should know how to seek support and should understand that they will not be in trouble for asking for help, either at school or with the police, if an image of themselves has been shared. Pupils should also understand that sharing indecent images of people over 18 without consent is a crime
- › What to do and how to report when they are concerned about material that has been circulated, including personal information, images or videos, and how to manage issues online
- › About the prevalence of deepfakes including videos and photos, how deepfakes can be used maliciously as well as for entertainment, the harms that can be caused by deepfakes and how to identify them
- › That the internet contains inappropriate and upsetting content, some of which is illegal, including unacceptable content that encourages misogyny, violence or use of weapons. Pupils should be taught where to go for advice and support about something they have seen online. Pupils should understand that online content can present a distorted picture of the world and normalise or glamorise behaviours which are unhealthy and wrong
- › That social media can lead to escalations in conflicts, how to avoid these escalations and where to go for help and advice
- › How to identify when technology and social media is used as part of bullying, harassment, stalking, coercive and controlling behaviour, and other forms of abusive and/or illegal behaviour and how to seek support about concerns
- › That pornography, and other online content, often presents a distorted picture of people and their sexual behaviours and can negatively affect how people behave towards sexual partners. This can affect pupils who see pornographic content accidentally as well as those who see it deliberately. Pornography can also portray misogynistic behaviours and attitudes which can negatively influence those who see it
- › How information and data is generated, collected, shared and used online

- › That websites may share personal data about their users, and information collected on their internet use, for commercial purposes (e.g. to enable targeted advertising)
- › That criminals can operate online scams, for example using fake websites or emails to extort money or valuable personal information. This information can be used to the detriment of the person or wider society. About risks of sextortion, how to identify online scams relating to sex, and how to seek support if they have been scammed or involved in sextortion
- › That AI chatbots are an example of how AI is rapidly developing, and that these can pose risks by creating fake intimacy or offering harmful advice. It is important to be able to critically think about new types of technology as they appear online and how they might pose a risk

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

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and pupils with SEND. Adaptations may include developmentally appropriate teaching, alternative or augmentative communication and recognition that pupils who cannot verbally report online harm may communicate distress through their behaviour.

4.2 Pupils will be taught practical cyber security skills

All pupils will receive age-appropriate training on safe internet use, including:

- › Methods that hackers use to trick people into disclosing personal information
- › Password security
- › Social engineering
- › The risks of removable storage devices (e.g. USBs)
- › Multi-factor authentication
- › How to report a cyber incident or attack
- › How to report a personal data breach

Pupils will also receive age-appropriate education on safeguarding issues such as cyberbullying and the risks of online radicalisation.

5. Educating parents/carers about online safety

The school will raise parents/carers' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents/carers.

Online safety will also be covered during parents' evenings.

The school will let parents/carers know:

- › What systems the school uses to filter and monitor online use
- › What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the 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 1 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 encourage them 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. Teachers will discuss cyber-bullying with their classes at an age appropriate level.

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, proprietary board 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/carers so 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

Pupils at Serenity School are not permitted to carry personal electronic devices in school (e.g., mobile telephones). If it is suspected that a pupil has brought a second device to school, the headteacher, and any member of staff authorised to do so by the headteacher, can carry out a search and confiscate the device. Please see Searching, screening and confiscation in the Behaviour policy.

6.4 Artificial intelligence (AI)

Generative AI tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Gemini.

Serenity School recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

Serenity School will treat any use of AI to bully pupils very seriously, in line with our Anti-Bullying and Harassment policy.

Staff should be aware of the risks of using AI tools while they are still being developed and should carry out a risk assessment where new AI tools are being used by the school, and where existing AI tools are used in cases which may pose a risk to all individuals that may be affected by them, including, but not limited to, pupils and staff.

When introducing generative AI products, Serenity Schools will assess the associated safeguarding risks with reference to the DfE's Generative AI product safety standards.

Any use of artificial intelligence should be carried out in accordance with our Artificial Intelligence policy.

7. Acceptable use of the internet in school

All parents/carers, staff, volunteers and the proprietary board are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 to 3). Parents undertake this signing on behalf of their child. Visitors will be expected to read and agree to the school's terms on acceptable use, when relevant.

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, the proprietary board and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate.

8. Pupils using mobile devices in school

Pupils may bring mobile devices to school e.g., for use during the journey to and from school, but all devices are removed at the school gate. Pupils are not permitted to use a device during the school day.

9. Staff using work devices outside 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 can be made up of 3 random words, in combination with numbers and special characters if required, or generated by a password manager
- › 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
- › 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 by promptly installing the latest updates

Staff members must not use the device in any way that would violate the school's terms of acceptable use.

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 Techlogic IT Services or from their line manager.

10. 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 and ICT acceptable use. 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 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 that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Training for staff, proprietary board and volunteers

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, threatening, 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 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.

The proprietary board 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.

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. Serenity Schools utilises SENSO monitoring software across its schools to support the safeguarding of pupils when using school devices and systems. SENSO provides proportionate monitoring of online activity and generates alerts where there may be concerns relating to pupil safety, wellbeing, inappropriate content, self-harm, bullying, extremism or other safeguarding risks. Alerts will be reviewed promptly by appropriately trained staff. High-risk alerts will be escalated immediately to the DSL. Actions taken and outcomes will be recorded in accordance with the school's safeguarding procedures. Monitoring arrangements operate alongside the Group's filtering systems and form part of Serenity's wider safeguarding and online safety framework.

This policy will be reviewed every year by the Group Safeguarding Lead. At every review, the policy will be shared with the proprietary board. The review (such as the one available [here](#)) will 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.

The annual filtering and monitoring review will consider the school's pupil risk profile, including pupils' age, developmental understanding, SEND, communication needs and use of assistive technology. It will also consider how generative AI is used and whether the school's systems can appropriately filter or monitor real-time, dynamic, personalised and AI-generated content. The review will cover relevant devices and locations, and its findings and resulting actions will be recorded.

13. Links with other policies

This online safety policy is linked to our:

- › Child protection and safeguarding policy
- › Behaviour policy
- › Staff disciplinary procedures

- › Data protection policy and privacy notices
- › Complaints procedure
- › ICT and internet acceptable use policy

Appendix 1: online safety training needs – self-audit for staff

Schools may use this form at induction to ascertain individual staff member needs.

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	Date:
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, The proprietary board and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents/carers?	
Are you familiar with the filtering and monitoring systems on the school's devices and networks?	
Do you understand your role and responsibilities in relation to filtering and monitoring?	
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?	