Compass Eko

Trust

Online Safety

Monitoring, evaluation and review

The Board of Trustees will assess the implementation and effectiveness of this policy. The policy will be promoted and implemented throughout all Trust schools.

This Policy will be reviewed by the Board of Trustees on a yearly cycle.

Adherence to the policy will be monitored by the Local School's Committee.

Policy adopted:	Spring Term 2026
Aligned	Rowan Wood School
Other related policies:	• Safeguarding and child protection • Behaviour and relationships • AI policy • Code of conduct • Personal devices • Staff disciplinary procedures • Data Protection Policy and privacy notices • Complaints procedure • Induction
Next Review:	Spring Term 2027

Contents

Aims 4

The four Key Categories of risk 4

Legislation and guidance 5

Roles and responsibilities 5

Filtering and monitoring 8

Educating Pupils about online safety 9

In partnership with parents 12

Online Risks 12

Examining electronic devices 13

Artificial Intelligence 14

Acceptable Use.....14

Remote learning 15

Pupil use of mobile phones / devices in school 15

Training 15

Appendices 17

Aims

At the Compass Eko Trust, we aim to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers, trustees 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
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate
- Identify and support groups of pupils that are potentially at greater risk of harm online than others
- Ensure a whole-school safeguarding approach where online safety is fully integrated into child protection practice, the curriculum offer and wider opportunities and experiences.

The Four key categories of risk

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

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism, misinformation, disinformation (including fake news) and conspiracy theories.
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

We recognise that these categories increasingly overlap and alongside other wider safeguarding issues (e.g. AI-enabled abuse, coercion linked with financial exploitation), and staff will consider contextual safeguarding risks when assessing concerns

Legislation and guidance

This policy is based on statutory safeguarding guidance including Keeping Children Safe in Education which strengthens expectations around:

- Early help and contextual safeguarding (including online contexts)
- Low-level concerns and staff conduct online
- Harmful sexual behaviour taking place online
- Use of emerging technologies including artificial intelligence
- Filtering and monitoring roles and accountability

This policy should be read alongside Part 1 and Annex B of KCSIE 2026.

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 and our funding agreement and articles of association.

- Teaching online safety in schools
- Preventing and tackling bullying
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education - We are mindful that this document is currently under review
- Searching, screening and confiscation
- Generative artificial intelligence in education
- DfE's non-statutory cyber security standards for schools and colleges.

It also refers to up to date guidance on Prevent duty guidance: England and Wales (2023) - GOV.UK (www.gov.uk).

Roles and responsibilities

Trust Board

The Trust Board has overall responsibility for:

- Reviewing filtering and monitoring standards

- Reviewing filtering and monitoring annually
- Blocking harmful content
- Having effective monitoring strategies in place to enable safe, effective systems
- A named safeguarding governor takes strategic responsibility for online safety
- Regular assurance that safeguarding (including online safety) is effective through triangulation of data, safeguarding reports and staff voice
- Appropriate oversight of the use of AI and emerging technologies in the Trust

Local School Committees / Governors

- Monitoring effectiveness of this policy
- Co-ordinating regular meetings with appropriate staff to discuss online safety and monitor online safety training logs as provided by the designated safeguarding lead (DSL).
- Ensuring online safety is considered within wider safeguarding audits and reviews
- Ensuring that safeguarding practice reflects local contextual risks including those arising online (e.g. community-based risks, exploitation, county lines)
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children and those with SEND, in recognition that a one size fits all approach may not be appropriate for all situations and a more personalised, contextualised approach may be more suitable.
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet
- Ensuring appropriate filtering and monitoring systems are in place and review their effectiveness

The Director of IT Strategy, Infrastructure and Communications is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Ensuring the school's network is constantly monitored by LGFL.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.

Headteacher

- Ensuring staff understand and implement the policy
- Ensuring filtering and monitoring systems are effective
- Responding to safeguarding concerns
- Logging incidents
- Ensuring a culture of vigilance where online safety concerns are identified early and acted upon
- Ensuring staff understand how to report both safeguarding concerns and low-level concerns related to online behaviour (including staff conduct)
- Ensuring safer recruitment and staff behaviour expectations extend to online conduct
- Liasing with other / external agencies as required
- Ensure the curriculum pupils receives enables them to understand how to keep themselves safe online
- Ensure all staff have received appropriate training and updates as required to support pupils effectively
- Enabling Governors to undertake their role in monitoring this area effectively, utilising the appropriate audit tool guidance
- Working with the IT director to ensure appropriate systems are in place

The designated safeguarding lead (DSL) is responsible for:

- Supporting the Head Teacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Taking lead responsibility for understanding and responding to online harms, including:
    - online sexual abuse and harassment
    - child criminal exploitation facilitated online
    - AI-generated harm (e.g. deepfakes)
- Ensuring that online safety concerns are considered within early help assessments and multi-agency work
- Maintaining oversight of patterns/trends in online incidents to inform safeguarding practice
- Ensuring that any online safety including cyber-bullying incidents are logged and dealt with appropriately
- Updating and delivering staff training on online safety (appendix 3 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services as necessary

- Providing regular reports on online safety in school to the headteacher and/or governing board
- Liaising with the trust Director of IT Strategy, Infrastructure and Communications to ensure appropriate filtering and monitoring systems are in place
- Ensuring all staff understand their expectations, roles and responsibilities in relation to filtering and monitoring

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

- Maintaining an understanding of and implementing this this policy
- Understand that safeguarding incidents can occur online and outside school, and may require action
- Maintain appropriate professional boundaries online in line with staff code of conduct
- Report low-level concerns relating to staff online behaviour in line with Trust procedures
- Agreeing and adhering to the terms on acceptable use of the School's ICT systems and the internet (Appendix 1), and ensuring that pupils follow the school's terms on acceptable use
- Working with the DSL to ensure that any online safety or cyber incidents are logged and dealt with appropriately in line with this policy

Parents

Parents are expected to:

- Notify a member of staff or the Head Teacher of any concerns or queries
- Ensure their child has read, understood and agreed to the terms on acceptable use of the School's ICT systems and internet (appendix 1)

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 factsheet - Childnet International

Filtering and Monitoring

We subscribe to WebScreen (LGFL).

- Filtering and monitoring is part of a wider safeguarding system and not solely a technical solution
- All staff understand thr role in responding to alerts and concerns

- Filtering systems are regularly reviewed for effectiveness and appropriateness to age and risk
- Monitoring systems actively identify safeguarding risks (not just technical breaches)

Educating pupils about online safety

We ensure pupils are sequentially taught:

- How to recognise online coercion, manipulation and exploitation
- The risks of AI-generated content and misinformation
- How to seek help and report concerns confidently
- Healthy digital behaviours and digital resilience
- That online abuse is taken as seriously as offline abuse

Our approach to educating pupils is drawn directly from Teaching online safety in schools - GOV.UK (www.gov.uk).

Pupils in **EYFS** will be taught about online safety as part of provision focused on the development of Personal, Social and Emotional Development (PSED)

Pupils in Key stage 1 and 2 will be taught about online safety as part of the curriculum:

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

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

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

- 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.
- 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.

- 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 risks, harmful content and contact, and how to report them
- 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
- How information and data is shared and used online

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

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

The School will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

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.

In partnership with parents

The school will support parents' awareness of internet safety in letters or other communications home, including emerging risks (AI, new platforms and online trends) and in information via websites. We will also support parents to understand their role in safeguarding children online beyond the school environment.

This policy will also be shared with parents.

The National College platform is available to offer guidance and support to parents and carers

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

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

Online Risks

Content, Conduct, Commerce, and Contact risks including cyber- bullying take place online, such as through social networking sites, messaging apps, gaming sites and occur through emerging technologies including AI and CSAM / deepfake content.

Online Risks also link *to* harmful sexual behaviour, peer-on-peer abuse or exploitation.

See also the school behaviour and relationship policy.

Preventing and addressing online issues including cyber bullying

To help prevent risks from online issue, 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 online safety with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover Online safety. This includes Relationships and Sex Education (RSE) education, and other subjects where appropriate.

In relation to a specific incident of Online safety, the school will follow the processes set out in the school **Behaviour and Relationships and Safeguarding and Child Protection policies**. 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.

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 hold for the purposes of evidence for other professionals and personal / wearable devices including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so. The decision to search must be made by the headteacher/deputy headteacher or DSL.

When deciding whether there is a good reason to examine 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 or poses risk, and/or
- Disrupt teaching, and/or
- Break any of the school rules / commit an offence

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

- Make an assessment on how urgent the search is
- Seek cooperation from the individual

If inappropriate material is found on the device, it is up to the conjunction with the DSL or head teacher to decide whether they should, first from a safeguarding perspective, whether to:

- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police
- Delete that material, only where appropriate

If a staff member suspects a device may contain an intimate image of a child, they will:

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

Any searching of pupils will be carried out in line with the DfE's latest guidance on searching, screening and confiscation. Searching, screening and confiscation in schools - GOV.UK. Any searches undertaken must be logged. Please see procedures set out in our behaviour and relationship policy. Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

Artificial Intelligence (AI)

Generative artificial intelligence (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 Bard.

We recognise 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.

We will treat any use of AI to bully pupils in line with our anti-bullying/behaviour policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used.

Acceptable use

All pupils, parents, staff, volunteers, trustees, and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (Appendices 1 and 2). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant. This will be done via the schools' sign in systems if they have them or on paper in their absence.

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, trustees, governors and visitors (where relevant) to ensure they comply with the above.

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

Remote Learning

The online learning platforms we use are safe and secure and can only be accessed by the child and class teacher.

If online learning includes any form of live streaming/videoing teachers must:

- ensure parental consent has been obtained
- be mindful of their surroundings, ensuring any personal photos etc are not in view
- consider background noise that may be heard by children
- ensure others who they may live with are not present in the room during lessons
- ensure they dress appropriately for school
- ensure they are in control of the screen
- save the video/chat content

Pupils using mobile devices / phones in school

Pupils who travel to school unaccompanied may bring mobile devices to school, but are not permitted to use them during the school day.

Mobile phones must be handed to school staff and stored safely during the school day.

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 as part of their induction. Volunteers will receive appropriate training and updates.

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).

The DSL's 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 and trustees will receive training on safe internet use and online safeguarding issues as part of their annual safeguarding training.

Further information about safeguarding training is set out in our child protection and safeguarding policy.

APPENDIX 1: The Compass Eko Trust

Acceptable Use of Internet and Digital Technologies Staff / volunteers / Governor / Trustee Agreement

All adults within the school must be aware of their safeguarding responsibilities when using any online technologies, such as the internet, E-mail or social networking sites. They are required to sign this Acceptable Use Agreement before being allowed access to these technologies.

- I know that I must only use school equipment and internet connection in an appropriate manner and for professional uses, and that my usage is subject to monitoring and review.
- I understand that I should act as a role model to children and young people for the safe and responsible use of the internet and digital technologies and will not use them in any way that could cause reputational damage.
- I understand that I should ensure children are accessing technology and online content appropriate for their age or stage.
- I understand that I need to obtain parental permission for children and young people before I or they can upload images (video or photographs) of themselves to the internet or send them via E-mail.
- I know that images should not be inappropriate or reveal any personal information of children and young people.
- I have read the procedures for incidents of misuse or online safety in the online safety policy so that I can deal with any problems that may arise, effectively.
- I will report accidental misuse.
- I will report any incidents of concern for a child or young person's safety to the designated online safety officer / DSL (or head teacher in their absence) in accordance with procedures listed in the online safety policy.
- I know who my designated online safety officer / DSL is.
- I understand the risks involved should I contact children and young people via personal technologies, including my personal e-mail, such as misinterpretation and allegations.
- I know I should use the school e-mail address and phones to contact parents.
- I know that I must not use the school IT systems for personal use unless this has been agreed by the Headteacher.

- I know that I should ensure that devices I use in school have adequate anti-virus and/or anti-malware protection so that I do not inadvertently transfer viruses, especially where I have downloaded resources.
- I will ensure that I follow the General Data Protection Regulations (2018), have read the Trust Data Protection Policy and have checked I know what this involves.
- I will ensure that I keep all passwords secure and not disclose any security information without head teacher approval. If I feel someone inappropriate requests my password I will report this to my head teacher.
- I will adhere to copyright and intellectual property rights.
- I will always log off or shut down a computer when I've finished working
- I will not open attachments in emails, or follow any links in emails that cause concern and will speak to my head where they do
- I will not use any personal device on school premises, without the approval of the headteacher
- I will only install and use hardware and software I have been given permission for.
- I accept that the use of any technology designed to avoid or bypass the school filtering system, such as tethering to a mobile phone or a mobile WIFI hotspot is prohibited, unless explicit permission is given by a headteacher or member of the executive leadership team.

- I have been shown a copy of the Online Safety Policy to refer to about all online safety issues and procedures that I should follow. A copy can be found on the school website.

I have read, understood and agree with these Agreements as I know that by following them I have a better understanding of Online Safety and my responsibilities to safeguard children and young people when using online technologies and the reputation of the school and Trust.

Signed……. Date…….

Name (printed)…….

APPENDIX 2 - Model Acceptable Use of Internet and Digital Technologies Pupil Agreement

This should be adapted to be age / level appropriate, so that the children signing can understand what is being agreed

Our Charter of Good Online Behaviour

I Promise – to only use the school IT for schoolwork that the teacher has asked me to do.

I Promise – not to look for or show other people things that may be upsetting.

I Promise – to show respect for the work that other people have done.

I will not – use other people's work or pictures without permission to do so.

I will not – damage the IT equipment, if I accidentally damage something I will tell my teacher.

I will not – share my password with anybody. If I forget my password, I will let my teacher know.

I will not – use other people's usernames or passwords.

I will not – share personal information online with anyone.

I will not – download anything from the Internet unless my teacher has asked me to.

I will – let my teacher know if anybody asks me for personal information.

I will – let my teacher know if anybody says or does anything to me that is hurtful or upsets me.

I will – be respectful to everybody online; I will treat everybody the way that I want to be treated.

I understand – that some people on the Internet are not who they say they are, and some people can be nasty. I will tell my teacher if I am ever concerned in school, or my parents if I am at home.

I understand – that my school will monitor the websites I visit.

I understand – if I break the rules in this charter there will be consequences of my actions and my parents will be told.

Signed (Parent) :

Signed (Child) :

Date :

Appendix 3: Audit for staff

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 child 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?	