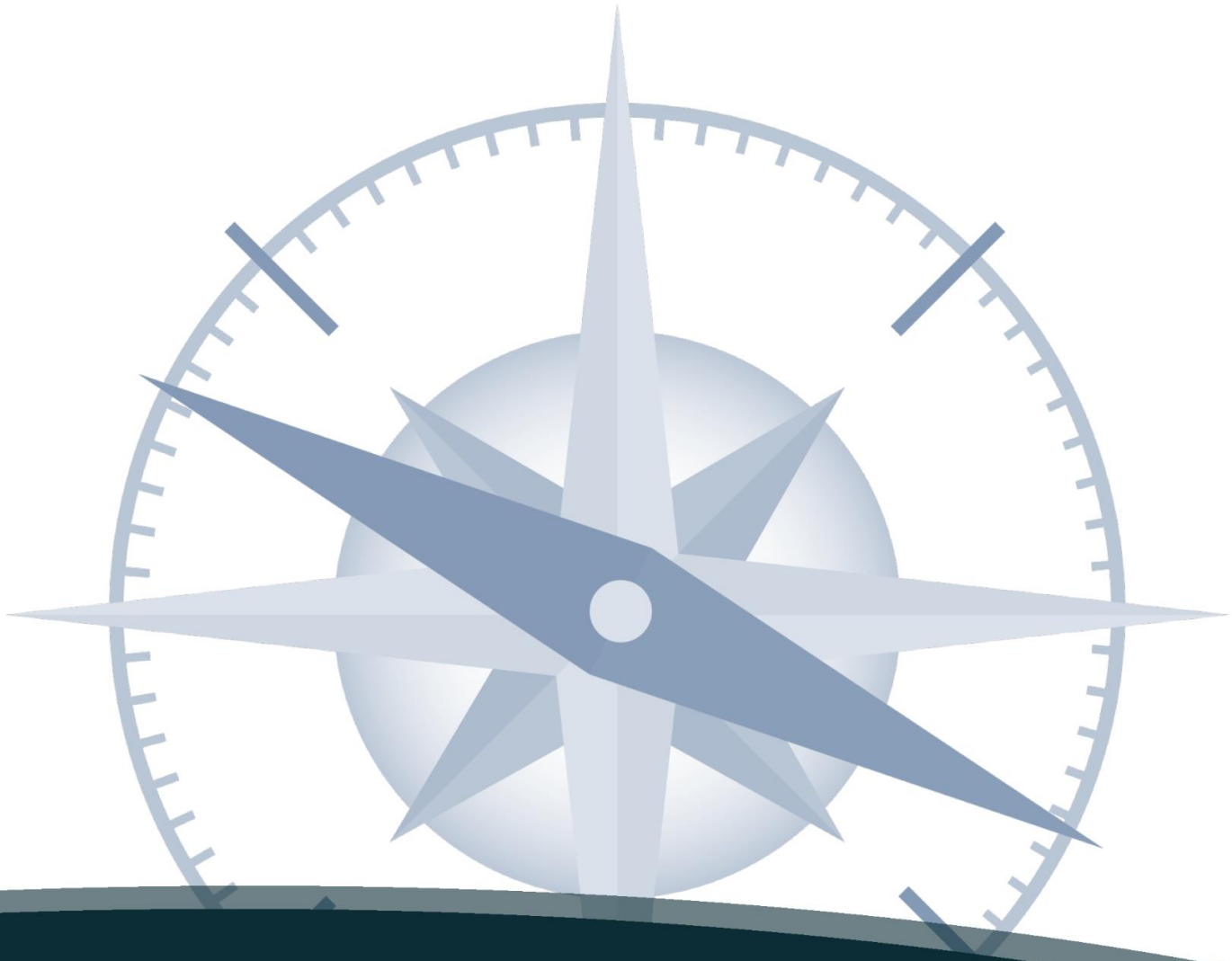

Online Safety

THE COMPASS
PARTNERSHIP OF SCHOOLS

At the Compass Partnership of Schools 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

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
- 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 Department'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.

Roles and responsibilities

The Local School Committee has overall responsibility for:

- monitoring this policy and holding the headteacher to account for its implementation.
- co-ordinating regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL). Please see appendix 4 for support

The Head teacher is responsible for:

- ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

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

- Working with the Head Teacher, The Director of IT Strategy, Infrastructure and Communications and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged using my concern and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged using my concern and dealt with appropriately in line with the school behaviour policy
- 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

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.

All staff, contractors, 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 1), and ensuring that pupils follow the school's terms on acceptable use
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- This list is not intended to be exhaustive.

Parents

Parents are expected to:

- Notify a member of staff or the Head Teacher 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 (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\\

Educating pupils about online safety

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:

- 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
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

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

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.

Educating parents about online safety

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

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.

Cyber-bullying

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 and relationship policy*.

Preventing and addressing cyber-bullying

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

The School will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes Relationships and Health Education (RHE) education, and other subjects where appropriate.

All staff receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour and relationships. 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, 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. The decision to search must be made by the headteacher/deputy headteacher or DSL.

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 inappropriate material is found on the device, it is up to the conjunction with the DSL or head teacher to 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

Any searching of pupils will be carried out in line with the DfE's latest guidance on searching, screening and confiscation.
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1091132/
Searching__Screening_and_Confiscation_guidance_July_2022.pdf

Any searches undertaken must be logged on my concern. 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.

Acceptable use of the internet in school

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 (appendices1 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 in school

Pupils who travel to school unaccompanied may bring mobile devices into 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

Staff using work devices outside school

Please see the Compass Equipment Loans Policy.

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.

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.

Volunteers will receive appropriate training and updates, as applicable.

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

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 annually or earlier if a major incident occurs.

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

Policy adopted:	Autumn Term 2022
Other related policies:	• Safeguarding and child protection • Behaviour and relationships • Staff disciplinary procedures • Data protection policy and privacy notices • Complaints procedure • Induction
Next Review:	Autumn Term 2023 Or before if statutory guidance changes

APPENDIX 1: The Compass Partnership of Schools
Acceptable Use of Internet and Digital Technologies Staff 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 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.
- 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 (or head teacher in their absence) in accordance with procedures listed in the online safety policy.
- I know who my designated online safety officer 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 MAT 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 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 forbidden without head teacher approval. I understand that intentional violation of this rule may result in disciplinary procedures being initiated.
- 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.

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?	
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?	

Appendix 4: Online safety in schools: Questions from the Local School Committee

Children have the right to enjoy childhood online, to access safe online spaces, and to benefit from all the opportunities that a connected world can bring to them, appropriate to their age and stage.

The Department for Education's Keeping Children Safe in Education statutory guidance states that, "Governing bodies and proprietors should ensure that children are taught about safeguarding, including online safety. Schools and colleges should consider this as part of providing a broad and balanced curriculum. This may include covering relevant issues through Relationships Education and Relationships and Sex Education. Personal, Social, Health and Economic (PSHE) education."

Question	Is there an up to date online safety policy/acceptable use policies in place? How does the school assess that it is clear, understood and respected by all children and staff?
Why this question?	The Department for Education's (DfE) 'Keeping Children Safe in Education' (KCSIE) statutory guidance states that "Governing bodies and proprietors should ensure there are appropriate procedures in place...to safeguard and promote children's welfare... this should include ... acceptable use of technologies...and communications including the use of social media." Annex C KCSIE also states that 'Governors and proprietors should consider a whole school/college approach to online safety. This will include a clear policy on the use of mobile technology in the school.' The 2019 DfE guidance document 'Teaching online safety in schools' states that schools should create "a culture that incorporates the principles of online safety across all elements of school life. The principles should be reflected in the school's policies and practice where appropriate, and should be communicated with staff, pupils/students and parents. This will include, for example, in the child protection policy clear processes for reporting incidents or concerns."
What to look for	• .Systematic and regular review of safeguarding policies, including online safety, at least on an annual basis. • Evidence that online safety policies are readily available • Pupils, staff and parents are aware of online safety rules and expectations
What is good practice	• Collaborative production and review of policies, for example, evidence of the active use of pupils' and parents' views. • Evidence of monitoring and evaluation processes to ensure understanding of, and adherence to, online safety policies. • Pupils, staff and parents are aware of online safety behaviour and expectations, including the acceptable use of technologies and the use of mobile technology.

	• The school safeguarding policy recognises peer on peer abuse concerns which can take place online. • Linked to and a part of other policies, such as safeguarding and child protection,
Question	What mechanisms does the school have in place to support pupils staff and parents facing online safety issues?
Why this question?	The 2019 DfE guidance document 'Teaching online safety in schools' states that "It is important to create a safe environment in which pupils/students feel comfortable to say what they feel. If a pupil /student thinks they will get into trouble and/or be judged for talking about something which happened to them online they may be put off reporting it and getting help" and "it is essential all pupils/students are clear what the school's reporting mechanisms are". With regards to monitoring and filtering, the KCSIE statutory guidance states "As schools and colleges increasingly work online it is essential that children are safeguarded from potentially harmful and inappropriate online material. As such governing bodies and proprietors should ensure appropriate filters and appropriate monitoring systems are in place."
What to look for	• Online safety clearly recognised as a safeguarding issue within the roles and responsibilities of all staff in the school with overall responsibility held by the Designated Safeguarding Leads (DSL). • Whole school approach, in which robust reporting channels are well-defined, clearly understood and consistent and known by staff, pupils/students and parents. • Clearly described procedures for responding to different online harms (e.g. Sharing of indecent images; Online Bullying and Online grooming etc.) • Links into other relevant policies and procedures e.g. whistleblowing/managing allegations, complaints etc. • Leadership staff are aware of and understand the decisions made by the school in respect to implementing 'appropriate filtering and monitoring'. • Regular review of monitoring and filtering provisions as part of safeguarding
What is good practice?	• Online reporting mechanisms for pupils and parents. • All staff are aware of sources of support for online safety issues, such as the Professionals Online Safety Helpline, Reporting Harmful Content, CEOP and Internet Watch Foundation. https://www.saferinternet.org.uk/helpline/professionals-online-safety-helpline https://www.saferinternet.org.uk/helpline/report-harmful-content https://www.ceop.police.uk/ceop-reporting/ https://report.iwf.org.uk/en

	• DSL's have the appropriate skills and are trained to deal with the various risks related to online activity. There may be additional nominated members of staff who support this area with their expertise. • All staff should receive appropriate safeguarding and child protection training, including online safety (as set out in KCSIE). • Planned and effective peer support strategies, e.g. reporting mechanisms/escalation processes • Auditing of online behaviour and harms which provides base line information from the pupils/ about the levels and types of online issues prevalent in the school/college. • Regular evaluation of reporting channels and response procedures. • Online safety information/data highlighted within the Head Teacher's report to the Governing body. • Appropriate filtering and monitoring decisions are regularly reviewed in line with the school/college's needs and relevant information is clearly communicated to staff, pupils/students and parents.
Question	How do you ensure that all staff receive appropriate, relevant and regularly updated online safety training?
Why this question?	The KCSIE statutory guidance states that "all staff undergo safeguarding and child protection training (including online safety) at induction" and that "online safety training for staff is integrated, aligned and considered as part of the overarching safeguarding approach". Annex B KCSIE statutory guidance states that DSLs should ensure that 'they are able to understand the unique risks associated with online safety", are "confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online at school or college" and that they "can recognise the additional risks that children with SEN and disabilities (SEND) face online". The DfE guidance document 'Teaching online safety in schools' states that "school staff have access to up to date appropriate training/CPD and resources, so that they are confident in covering the required content in a way that is relevant to their pupils/students' lives."
What to look for	• Training which improves staff knowledge of, and expertise in, safe behaviours and appropriate use of technologies. • Audit of the training needs of all staff. • Online safety training as an integral part of the required, at least annual, safeguarding training for all staff. Online safety training as an integral part of induction for all new staff. • Online safety training coordinated by the DSL. • Evidence that the DSL has ensured that their knowledge and skills regarding online safety is robust. .

What is good practice	• DSL's have a higher level of training, knowledge and expertise on online safety issues, with clearly defined responsibilities related to online safety provision for the school community. • Expertise in online safety is developed across a pool of staff, to ensure transfer and sustainability of knowledge and training. • Online safety training clearly established within the school wider safeguarding training. • Training content updated to reflect current research and advances in technology as well as local policy and procedures. • Online safety training is given to all new staff as part of induction.
Question	Describe how your school provides the learning required to educate children and young people to build knowledge, skills and confidence with regard to online safety. This will included learning contained within the statutory (September 2020) Relationships Education, Relationships and Sex Education (RSE) and Health Education, the Computing curriculum, Citizenship and other subjects where relevant.
Why this question?	In England, from September 2020, Relationships Education will be compulsory for all primary aged pupils and Relationships and Sex Education compulsory for all secondary aged pupils[1]. Health Education will be compulsory for all pupils in state-funded schools[2]. Online safety education is embedded throughout these subjects. Children have a right to education about their rights across both online and offline contexts, as well as how to respect the rights of other online users. Children equally have a right to education which teaches them who to ask for help if things go wrong. The internet does not yet provide a safe and equal space for all children, and so they have a right to be taught how to best navigate potential risks online and to have their own safety strategies recognised and supported. Education alone does not protect children. Children are not responsible for their own abuse online or otherwise even if they do not follow the safety messages /education taught in schools and other settings.
What to look for	• Teaching draws from the DfE guidance 'Teaching online safety in schools' (June 2019) Teaching enables children and young people to achieve the learning outcomes described within the UK Council for Internet Safety (UKCIS) framework 'Education for a Connected World' (February 2018) • Planned online safety education programme which is: o Taught across all age groups and progresses as pupils/ grow and develop. o Regular as opposed to a one-off online safety session. o Supports pupils in developing strategies for navigating the online world. o Embedded across the curriculum. o Incorporates/makes use of relevant national initiatives and opportunities such as Safer Internet Day and Anti-bullying week.

	• Use of appropriate and up-to-date resources. • Resources, including visitors from external providers used appropriately to support and compliment internal provision. • Accessible to pupils/ at different ages and abilities, such as pupils/students with Special Educational Needs and Disabilities (SEND), or those with English as an additional language. • Pupils are able to recall, explain and actively use online safety education. • Teachers have access to appropriate training, ensuring expertise and understanding underpins their teaching.
What is good practice	• Online safety is embedded throughout the school/college curriculum. This means that the opportunity to develop the knowledge, skills and confidence of pupils, on issues related to online safety, are planned into all relevant lessons such as in RHE, including Relationships and Sex Education, citizenship and computing. • Regular review of the online safety curriculum to ensure its relevance to pupils/students. The school uses the Education for a Connected World framework to review and quality assure online safety education.
Question	How does the school/college educate parents and the whole school community with online safety?
Why this question?	The 2019 DfE document 'Teaching online safety in school' states that the school culture should "incorporate the principles of online safety across all elements of school life ... reflected in the school's policies and practice ... communicated with staff, pupils and parents." And "Schools should also ensure they extend support to parents, so they are able to incorporate the same principles of online safety at home."
What to look for	• Regular communication, awareness-raising and engagement on online safety issues and reporting routes, such as the school/college website and newsletters. • Regular opportunities for engagement with parents on online safety issues such as awareness workshops.
What is good practice	• Interactive engagement with parents, with the aim of building skills and confidence to support their children in dealing with online harms, as well as general awareness on online safety issues. • Regular and relevant online safety resources and sessions offered to parents. Relevant resources will tackle key online risks and behaviours displayed by pupils at different ages in the school. • Evidence of pupils/students educating parents. • Online safety information available in a variety of formats, such as for those with English as an additional language.