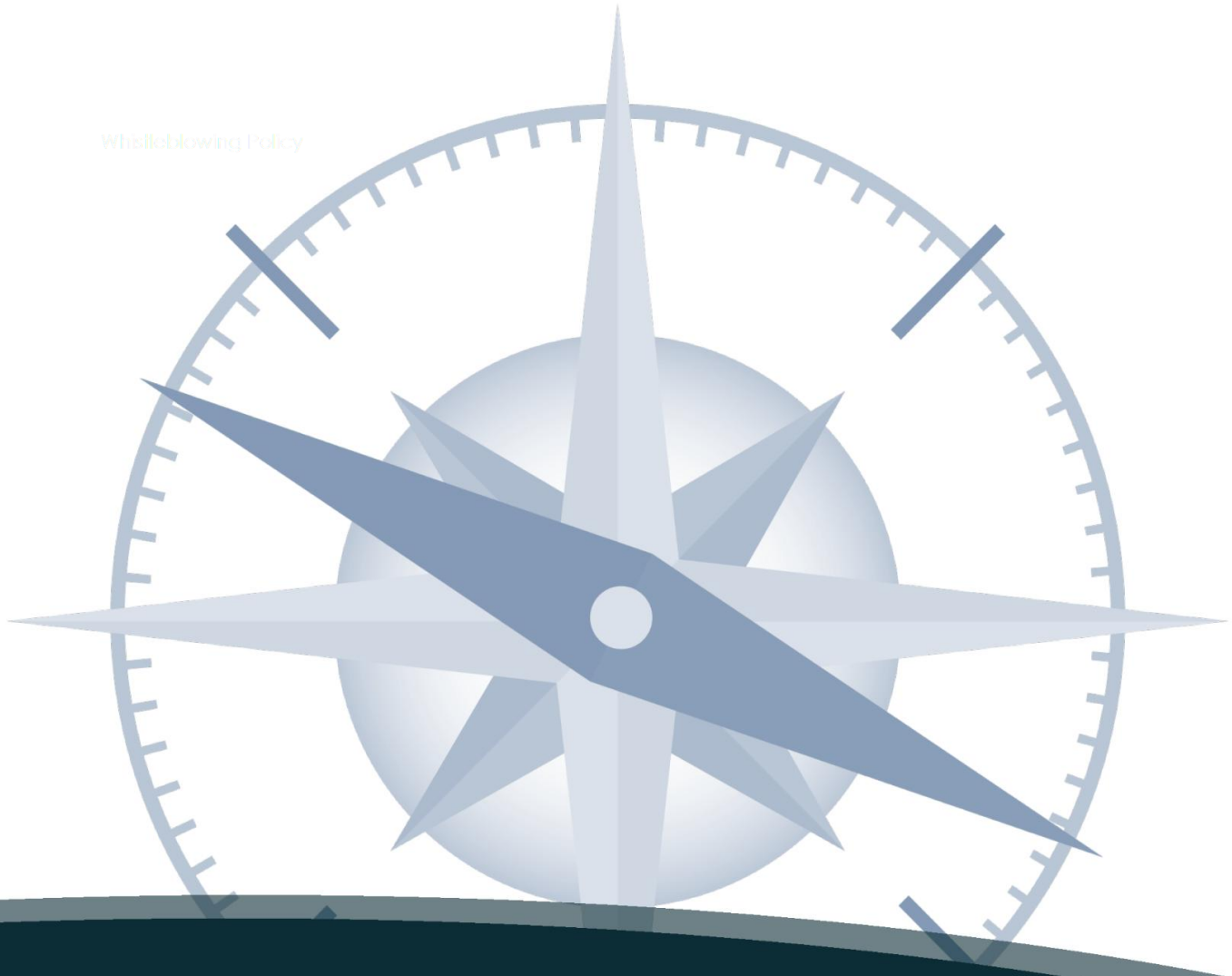

Online Safety Policy

THE COMPASS PARTNERSHIP OF SCHOOLS

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:	Summer Term 2025
Other related policies:	• Safeguarding and child protection • Behaviour and relationships • Staff disciplinary procedures • Data protection policy and privacy notices • Complaints procedure • Induction
Next Review:	Summer Term 2026 Or before if statutory guidance changes

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
- Identify and support groups of pupils that are potentially at greater risk of harm online than others

The 4 key categories of risk

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

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

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 - We are mindful that this document is currently under review
- Searching, screening and confiscation

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

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.

Roles and responsibilities

The Trust Board has overall responsibility for:

- Reviewing the Meeting digital and technology standards in schools and colleges - Filtering and monitoring standards for schools and colleges - Guidance - GOV.UK and discussing with IT leaders and service providers what needs to be done to support the school in the meeting the standards which include:
- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems
- Reviewing filtering and moniroting provisions at least annually
- Blocking harmful and inappropriate content with unreasonably impacting teaching and learning
- Having effective monitoring strategies in place that meet safeguarding needs.

The Local School Committee has overall responsibility for

- monitoring this policy and holding the headteacher to account for its implementation, using the appropriate audit tools.
- 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). Please see appendix 4 for support
- Ensuring pupils are taught how to keep themselves and others safe, including keeping safe online
- 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 Head teacher is responsible for:

- Ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.
- Ensuring appropriate filtering and monitoring systems are effective
- Ensuring all online safety issues and incidents in line with the Safeguarding policy
- Responding to all safeguarding concerns indentified by filtering and monitoring
- Ensuring that online safety incidents are logged
- 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
- 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
- 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

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\\

Filtering and Monitoring

We subscribe to Web screen (LGFL net.) Broadband and Beyond - WebScreen (lgfl.net) who monitor our systems on our behalf.

They conform to https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/cyber-security-standards-for-schools-and-colleges standards.

Any security breeches must be reported to our trust Director of IT Strategy, Infrastructure and Communications via the report button.

Educating pupils about online safety

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

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.
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.

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 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:

- 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

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

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

Any searching of pupils will be carried out in line with the DfE's latest guidance on searching, screening and confiscation. 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.

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 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.

APPENDIX 1: The Compass Partnership of Schools
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.
- 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 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 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 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 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 tteacher.
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?	