St Peter's CofE Primary, Whetstone

Online Safety Policy

2026 - 2028

Embrace Multi Academy Trust strives to maintain and improve good provision and outcomes at each of its member schools. Based upon our shared ethos and our values of wisdom, collaboration, respect, integrity, inclusivity, and compassion, we aim to support the learning and development of every person within the trust and our policies are written from this perspective.

Version	Approval Level	Document Status	Date Approved	Review Period	Next Review
V1	Trust Leader	Approved	27/08/2024	2 Years	
V2	Trust Leader	Approved	26/10/2026	2 Years	Sept 2028

Contents

1. Aims 3
2. Legislation and Guidance 3
3. Roles and Responsibilities 4
   - 3.1. The Local Governing Committee 4
   - 3.2. The Headteacher 4
   - 3.3. The Designated Safeguarding Lead (DSL) 4
   - 3.4. The Trust IT Manager 5
   - 3.5. Online Response Team 6
   - 3.6. All Staff and Volunteers 6
   - 3.7. Parents/carers 6
   - 3.8. Visitors and Members of the Community 6
4. Educating Pupils about Online Safety 7
5. Educating Parents/Carers About Online Safety 8
6. Cyber-bullying 8
   - 6.1. Definition 8
   - 6.2. Preventing and addressing cyber-bullying 9
   - 6.3. Examining electronic devices 9
   - 6.4. Artificial intelligence (AI) 9
7. Acceptable Use of the Internet in School 9
8. Pupils Using Mobile Devices in School 10
9. Staff Using Work Devices Outside of School 10
10. How the School will Respond to Issues of Misuse 11
11. Training 11
12. Monitoring Arrangements 12
13. Change Management Procedure 12
14. Procurement Procedure 13
15. Email Filtering 13
16. Links with Other Policies 13

Appendix 1: Online Safeguarding Action Plan 14

Appendix 2: Online Safety – Staff Audit 15

Appendix 3: Website Information 16

Version Updates 17

1. Aims

All schools within Embrace Multi Academy Trust aim to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers, and governors.
- Identify and support groups of pupils that are potentially at greater risk of harm online than others.
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones').
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

The 4 key categories of risk

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

- **Content** – being exposed to illegal, inappropriate, or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, and extremism.
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising, and adults posing as children or young adults with the intention to groom or exploit 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 (eg consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images, and online bullying.
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

2. Legislation and Guidance

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

- Teaching online safety in schools.
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff.
- Relationships and sex education
- Searching, screening and confiscation.

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study, the DfE Filtering and Monitoring Standards, the Online Safety Act 2023 and DfE guidance on generative artificial intelligence and data protection in schools.

This policy complies with our funding agreement and articles of association.

3. Roles and Responsibilities

3.1. **The Local Governing Committee**

Each school's local governing committee (LGC) has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

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

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

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

The LGC should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The LGC must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks and will regularly review their effectiveness. The LGC will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting those standards, which include:

- Each school identifying a senior leader with responsibility for filtering and monitoring. This individual will lead an annual review of effectiveness, supported by the DSL and IT staff.
- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems
- Reviewing filtering and monitoring provisions at least annually
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning
- Having effective monitoring strategies in place that meet their safeguarding needs.

The governor responsible for safeguarding will oversee online safety provision.

All governors will:

- Ensure they have read and understand this policy
- Agree and adhere to the acceptable use of IT policy for governors
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole school or college approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable.

3.2. **The Headteacher**

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3. **The Designated Safeguarding Lead (DSL)**

Details of each schools' DSL and deputy DSL(s) are set out in their child protection and safeguarding policy, as well as relevant job descriptions. The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school.
- Working with the headteacher and governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly.
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks, and ensuring the processes defined in the Online Safeguarding Action Plan (Appendix 1) are followed at all times.
- Working with the IT manager to make sure the appropriate systems and processes are in place.
- Working with the headteacher, IT manager and other staff, as necessary, to address any online safety issues or incidents.
- Managing all online safety issues and incidents in line with the school's child protection policy.
- Ensuring that any online safety incidents are logged (see Appendix 1)and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy.
- Updating and delivering staff training on online safety (Appendix 2 contains a self-audit for staff on online safety training needs).
- Liaising with other agencies and/or external services if necessary.
- Providing regular reports on online safety in school to the headteacher and/or governing board.
- Undertaking annual risk assessments that consider and reflect the risks children face.
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively.
- Ensuring annual filtering and monitoring reviews are recorded and reported to governors and trustees.

This list is not intended to be exhaustive.

3.4. **The Trust IT Manager**

The trust IT manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and ensure pupils are kept 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.
- Conducting a full security check and monitoring the school's ICT systems on a monthly basis.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.
- Ensuring that any online safety incidents are logged in line with the Online Safeguarding Action Plan (see appendix 1) 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.

3.5. **Online Response Team**

The Trust has a designated online response team who provide support in identifying and categorising online safety incidents. At school level, headteachers, DSLs and the pastoral teams review any potential online safety issue.

The online response team is responsible for:

- TRUST - Helping in the quick identification of safeguarding incidents, either from investigating automatically generated alerts or from proactive monitoring of the platform.
- TRUST/SCHOOL - Ensuring the information that has been identified is accurate.
- SCHOOL - Providing support and discussing situations of computer misuse with students to promote better decisions in the future.
- TRUST/SCHOOL - Closing any monitoring alerts which are not safeguarding related.

Any event which is deemed to be a safeguarding incident must be escalated to a DSL

3.6. **All Staff and Volunteers**

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

- Maintaining an understanding of this policy.
- Implementing this policy consistently.
- Agreeing and adhering to the acceptable use of IT policy for staff/volunteers and ensuring that pupils follow the acceptable use of IT policy for pupils.
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and ensuring any incidents of those systems or processes failing are promptly reported to them.
- Following the correct procedures by discussing needs with the IT team if they need to bypass the filtering and monitoring systems for educational purposes. A decision may need to be escalated to the DSL responsible.
- 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.
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'.

This list is not intended to be exhaustive.

3.7. **Parents/carers**

Parents/carers are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy.
- Ensure their child has read, understood and agreed to the acceptable use of IT policy (available on the Embrace MAT website).

Parents/carers can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International

3.8. **Visitors and Members of the Community**

Visitors and members of the community who use the school's IT systems or internet will be made aware of this policy and will be expected to read and follow it.

4. Educating Pupils about Online Safety

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

All schools have to teach:

- Relationships education and health education in primary schools
- Relationships and sex education and health education in secondary schools.

Pupils in Key Stage 1 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 online 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 it.
- How to critically consider their online friendships and sources of information, including awareness of the risks associated with people they have never met.
- How information and data is shared and used online.
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context).
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) and those whom they do not know.

Pupils in Key Stage 3 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 Key Stage 4 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:

- Their rights, responsibilities, and opportunities online, including that the same expectations of behaviour apply in all contexts, including online.
- About online risks, including that any material one person provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online.
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them.
- What to do and where to get support to report material or manage issues online.

- The impact of viewing harmful content.
- That specifically sexually explicit material (eg pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others, and negatively affect how they behave towards sexual partners.
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence that carries severe penalties including jail.
- How information and data is generated, collected, shared, and used online.
- How to identify harmful behaviours online (including bullying, abuse, or harassment) and how to report, or find support, if they have been affected by those behaviours.
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online).

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

Pupils will be taught, in an age-appropriate way, how to recognise and respond to misinformation and manipulated content, including deepfakes; understand how algorithms can influence the information and content they see; check the reliability, accuracy and source of online information; and use online platforms safely, responsibly and respectfully, including using privacy settings and reporting or blocking harmful or misleading content.

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

5. Educating Parents/Carers About Online Safety

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

Information provided to parents/carers will include guidance on age assurance, platform reporting functions and emerging online risks.

Some children may face increased online risk, including children with SEND, children in care, previously looked after children, children experiencing mental health difficulties and children vulnerable to exploitation.

The school will let parents/carers know:

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

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

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

6. Cyber-bullying

6.1. **Definition**

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group of people by another person or group of people, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

6.2. **Preventing and addressing cyber-bullying**

To help prevent cyber-bullying, our school 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. Class teachers and form teachers will discuss cyber-bullying with their tutor groups.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors, and volunteers (where appropriate) receive training on cyber-bullying, its impact, and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The school also sends information/leaflets on cyber-bullying to parents/carers so they are aware of the signs, how to report it, and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate, or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

6.3. **Examining electronic devices**

All schools will have clear and defined processes regarding how they carry out searches and confiscation of electronic devices if they have reasonable grounds for suspecting the device:

- poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- is evidence in relation to an offence.

These school specific approaches are defined in the examining electronic devices policy.

6.4. **Artificial intelligence (AI)**

The Trust recognises that artificial intelligence (AI), including generative AI, presents both opportunities and safeguarding risks. The use of AI by pupils, staff, governors and trustees is governed by the Trust Artificial Intelligence (AI) Policy. Any safeguarding concerns arising from AI use must be managed in accordance with both policies.

7. Acceptable Use of the Internet in School

All pupils, staff, volunteers, and governors are expected to sign an agreement regarding the acceptable use of IT policy (available on the Embrace MAT website). Visitors will be expected to read and agree to the school's terms on acceptable use of ICT systems and the internet, if relevant.

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

We will monitor the websites visited by pupils, staff, volunteers, governors, and visitors (where relevant) to ensure they comply with the above and will restrict access through filtering systems where appropriate.

8. Pupils Using Mobile Devices in School

Schools within Embrace MAT have the autonomy to make their own decisions about how and when mobile phones can be brought onto the school site. Information regarding these policies can be found in the student acceptable use of IT policy (available on the Embrace MAT website) and in the Trust mobile phone policy.

Any use of mobile devices in school by pupils must be in line with the school's acceptable use of IT agreement.

Any breach of the acceptable use of IT agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

9. Staff Using Work Devices Outside of School

All staff members will take appropriate steps to ensure their devices remain secure and detailed information on how work is to be conducted outside of school can be found in the staff acceptable use of IT policy. This includes, but is not limited to:

- Keeping the device password protected. Strong passwords are at least 10 characters long, with a combination of upper and lower-case letters, numbers and special characters (eg asterisk or currency symbol).
- This means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device.
- Making sure the device is locked when not in use or not with device.
- Not sharing the device among family or friends.
- Keeping operating systems up to date by always installing the latest updates.
- Returning the device on the request of the IT support team to carry out necessary updates and maintenance.

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

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the relevant IT manager.

Staff Online Conduct and Professional Boundaries

Staff must maintain appropriate professional boundaries in all online activity. Personal social media accounts must not be used to communicate with pupils, and staff must not accept or initiate connections with pupils through personal accounts. Communication with pupils must take place only through Trust-approved platforms, accounts and devices, for legitimate educational purposes and in accordance with the Staff Code of Conduct. Staff must not use personal messaging applications or private groups to contact pupils.

Staff are responsible for ensuring that their online activity, privacy settings and published content do not compromise their professional reputation, the reputation of the school or Trust, or the safety and wellbeing of pupils.

Any online harassment, abuse, impersonation, inappropriate contact or other safeguarding concern involving a pupil or member of staff must be preserved as evidence where safe to do so and reported promptly through the school's safeguarding and staff-reporting procedures.

10. How the School will Respond to Issues of Misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in both our behaviour management and student acceptable use of IT policies. The action taken will depend on the individual circumstances, nature, and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff code of conduct. The action taken will depend on the individual circumstances, and the nature and seriousness of the specific incident.

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

11. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues, including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins, and staff meetings).

All staff will receive online safety training at induction and at least annually thereafter. Training will ensure that staff understand their responsibilities for filtering and monitoring, including the purpose and limitations of the school's systems, how to recognise indications that filtering or monitoring may not be operating effectively, and how to report concerns or take immediate action where harmful content is accessed. Training will also reflect emerging online harms, including content promoting self-harm or eating disorders, harmful online challenges, and scams or other forms of financial exploitation, so that staff can recognise concerns, respond appropriately and follow the school's safeguarding procedures.

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse.
- Children can abuse their peers online through:
  - Abusive, harassing, and misogynistic messages.
  - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups.
  - Sharing of abusive images and pornography, to those who don't want to receive such content.
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element.

Training will also help staff to:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse.
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks.
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term.

The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

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

12. Monitoring Arrangements

The full process for ensuring monitoring is robust and effective, and details can be found in the IT Acceptable Use policy.

The school will review the effectiveness of its filtering and monitoring arrangements at least annually. The review will consider whether the systems remain appropriate to the school's context and risks, whether concerns and incidents have been identified and acted upon effectively, and whether staff understand their roles and reporting responsibilities.

The findings, agreed actions and evidence of follow-up will be recorded, retained and formally reported to the local governing committee and, where appropriate, the Trust.

An additional review will be undertaken following a significant safeguarding incident, a material change to technology or systems, the identification of a new or emerging online risk, or any concern that the existing arrangements may not be operating effectively.

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

13. Change Management Procedure

It is important any changes made to the filtering and monitoring platform undergo a rigorous change management process to ensure changes are not implemented which may impact student safety. Arrangements for these changes can be found below:

Filtering

- Requests for unblocking of websites and/or keywords are to be submitted by staff members using the online Microsoft Form.
- Requests are sent to the relevant DSL by the IT team with information about what the website is used for and the potential risks. The DSL risk assesses the website and decides whether to authorise the website/keyword or not.
- Where changes impact a larger number of schools (primary filtering, for example) notification is sent to all schools informing them of the change by the IT Team.
- IT implement the change, and changes are logged on a spreadsheet centrally including who approved the change.

Safeguarding Keywords

- There are occasions where keywords either need to be removed (eg generating too many false positives) or added (where a new trend is identified).
- Once a necessary change is identified, it is discussed with the trust safeguarding lead and risk assessed on a case-by-case basis.
- Change is implemented, if necessary, by the IT team and logged centrally, including the reason the change has been made and the name of the approver. The list of any changes are reviewed by the IT manager and Trust Safeguarding Improvement Lead.

14. Procurement Procedure

In addition to annual reviews of the effectiveness of the filtering and monitoring platform's effectiveness, it is important that DSLs, governors, and the IT Team carry out a thorough procurement process for filtering platforms to ensure that:

- The platform meets statutory guidance, including but not limited to KCSIE, PREVENT & Embrace Safeguarding Policy
- The platform supports all device types used across the trust.
- The platform is fit for purpose and provides the level of filtering and monitoring required for the school to effectively safeguard students.

Only once all parties are confident that the platform meets all the necessary requirements will a change to filtering or monitoring platforms be made.

15. Email Filtering

Where schools provide pupils with email accounts, a safeguarding keyword list is set on all pupil accounts to identify and filter a limited set of identified safeguarding keywords. When an email with a word on the safeguarding list is sent from a pupil account, a notification is sent to a member of the relevant IT team for approval.

This works in conjunction with any other safeguarding and monitoring tool and is primarily used to identify any areas of concern for pupils using email on an unmanaged, home device.

16. Links with Other Policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Staff code of conduct
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy

Appendix 1: Online Safeguarding Action Plan



Appendix 2: Online Safety – Staff Audit

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	**Date**:
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways pupils can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use of IT agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use of IT agreement for pupils and parents/carers?	
Are you familiar with the filtering and monitoring systems on the school's devices and networks?	
Do you understand your role and responsibilities in relation to filtering and monitoring?	
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 3: Website Information

Embrace Multi Academy Trust takes a holistic approach to online safety. By ensuring that we utilise the latest technology to help us identify areas of concern and educating all young people about the safe use of online platforms, we strive to ensure that all pupils are not only safe within school but have the knowledge and skills to navigate online risks outside of the school environment. Internet connections at our schools are filtered using Securly, ensuring that internet access is both filtered and monitored no matter what devices are used.

Pupil activity on devices within the school is also monitored using one of the leading cloud solutions, Classroom.Cloud by Netsupport. This safeguarding and monitoring software helps to proactively identify any areas of concern and ensure pupil safety and welfare is monitored at all times. Alerts proactively notify staff should a pupil be in crisis and our online response team and designated safeguarding leads are quick to provide the support necessary.

Online safety is covered extensively throughout our curriculum, both discreetly in the curriculum for IT and PSHCE, as well as being a regular topic for discussion in all curriculum areas.

If you have any concerns over electronic communication on any of these platforms, please do not hesitate to get in touch with the school on office@stpeters.embracemat.org

Version Updates

Version	Section	Update
2	2	Relationships and sex education added
	2	DfE Filtering & Monitoring Standards, Online Safety Act 2023, DfE AI guidance added
	3.1	New bullet point: identification of a senior leader for filtering & monitoring
	3.3	New bullet point: DSL to ensure annual filtering & monitoring reviews reported to governors/trustees.
	4	New para: areas pupils will be taught about in an age-appropriate way
	5	New paras: scope of information provided to parents & types of children facing increased online risks
	6.4	New bullet: AI
	9	New sub heading & content: staff online conduct and professional boundaries
	11	New para: Staff will receive online safety training at induction and at least annually thereafter
	12	New paras: i) annual review of effectiveness of filtering and monitoring. ii) findings reported to LGC. iii) circumstances in which an additional review will take place.