THE TWO COUNTIES TRUST

ONLINE SAFETY POLICY

Date of issue: 01/09/2023

1. Introduction

1.1 The Two Counties Trust recognises that if used correctly, technology can support and greatly enhance learning and communication. The use of technology can support the acquisition of powerful knowledge and encourage student independence.

1.2 As an organisation, the use of technology facilitates healthy and efficient communication and the sharing of ideas within and beyond our academies. All members of our organisation must understand what is meant by appropriate and inappropriate use of technology and the responsibility that comes with access to shared resources, including the internet.

1.3 Staff and students alike must appreciate that there can be risks and possible threats associated with online communication and that there is a clear expectation of conduct. Everyone must be mindful at all times of how their online conduct could negatively impact on others.

1.4 The Two Counties Trust is a values-driven organisation with highly professional relationships and diversity at its heart; we take seriously any wilful or unwitting damage to members of our community, or our reputation, caused by careless digital communication.

1.5 The Two Counties Trust is committed to providing a safe and secure environment for students, staff and visitors and promoting a climate where students and adults feel confident about sharing any concerns that they may have about their own safety or the wellbeing of others.

1.6 Filtering and monitoring practices and cyber security arrangements are in place in all academies which safeguard our students.

2. Scope and Purpose

2.1 This policy covers students, staff, visitors, governors, Trustees, and agency workers. Collectively they are referred to in this policy as employees or staff.

2.2 The policy should be read in conjunction with the following policies / documents:

- Anti-Bullying Policy
- Safeguarding and Child Protection Policy
- Behaviour Policy
- Conduct of Conduct
- Keeping Children Safe in Education (current version)
- Relationship and Sex Education Programme of Study
- Data Protection policy

2.3 This policy aims to educate the whole school community about their access to and use of technology and to establish effective mechanisms to identify, intervene and escalate incidents where appropriate.

2.4 Online safety covers the use of online platforms such as Microsoft Teams, the Internet, Social Media, e-mail and also the use of mobile phones and other electronic communication technologies.

2.5 This policy complies with all relevant legislation and statutory regulations and guidance, as updated and is published on the Trust website, and is available in hard copy on request.

3. Roles and Responsibilities

3.1 **Safeguarding Trustee**

The Safeguarding Trustee should receive assurances that:

- An online safety policy is in place and is available to all stakeholders.
- Designated Safeguarding Leads assume overall responsibility for online safety of students including lead responsibility for filtering and monitoring.
- All staff, trustees, and governors receive training and information on online safety, their roles and responsibilities.
- Procedures for the safe use of ICT and the Internet are in place and adhered to..

3.2 **Headteachers and Senior Leadership Teams, including the Designated Safeguarding Lead (DSL)**

The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the academy community.

Responsibility for online safety, including filtering and monitoring, is delegated to the Designated Safeguarding Lead who works with middle leaders in making sure there is a proactive programme of education in place. Any complaint about misuse must be referred to the Headteacher.

The Headteacher will work with the DSL and the Head of IT where appropriate in ensuring that:

- All staff and governors receive regular, up to date training both in educating young people, but also in relation to their own online conduct.
- Regular reviews of the online programme of study for young people are completed.
- Appropriate action is taken in all cases of misuse.
- Data Protection is taken seriously.
- Inappropriate use of IT is monitored, and that training is reviewed as appropriate.
- Filtering and monitoring reports are actioned appropriately.
- Reports about online safety issues are provided to the Safeguarding Governor.

3.3 **Head of Information Technology (IT)**

The Head of IT is responsible for ensuring that:

- Internet filtering and monitoring methods are appropriate, maintained, understood, effective and reasonable.
- the Trusts' technical infrastructure is secure and is not open to misuse or malicious attack.
- The online safety policy is current, relevant, and reflects risks associated with new technology.
- Users may only access the networks and devices through a properly enforced password protection policy.
- The filtering policy is applied and updated on a regular basis, at least annually, and its implementation is not the sole responsibility of any single person.
- Systems are in place to capture, record and flag to the Designated Safeguarding Lead early signs of harmful online behaviour or vulnerable students in each school.
- They keep up to date with online safety technical information to effectively carry out their online safety role and to inform and update others, including members of the IT team, as relevant.
- The use of all aspects of the network is regularly monitored in order that any misuse or attempted misuse is reported.
- Monitoring software and systems are implemented and updated regularly, at least annually, and in good time.

3.4 **School IT Support Team**

The school IT support teams will:

- Provide technical support to the Designated Safeguarding Lead, especially in the development and implementation of appropriate online safety practices and systems.
- Implement appropriate security measures (including password policies and encryption) to ensure that the school's IT infrastructure/systems are secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised without incurring risk to students.
- Ensure that the filtering policy is applied consistently and updated on a regular basis, at least annually, and that systems are in place to flag outputs to the Designated Safeguarding Lead.
- Report any filtering breaches to the Headteacher, Head of IT and the Designated Safeguarding Lead the school's web filtering provider or other services, as appropriate.
- Take personal responsibility for professional development in this area.

3.5 **Staff**

Staff members will:

- Know who the school's online safety lead is (the Designated Safeguarding Lead).
- Adhere to this policy and the Acceptable Use policy.
- Take responsibility for the security of school systems and the data they use or have access to.
- Model good practice when using technology and maintain a professional level of conduct in their personal use of technology, both on and offsite.
- Embed online safety education in curriculum delivery.
- Be alert to online risks and how they may be experienced by the children in their care and put steps in place to manage these risks in so far as possible.
- Escalate online safety concerns to the Designated Safeguarding Lead.
- Follow the safeguarding policy in respect of online safety.
- Report to the DSL and/or ICT Support team if they see or suspect unacceptable content is being or can be accessed, or if there is a failure of the filtering and monitoring system.
- Report to the DSL and/or ICT Support team if they expect the content, they are teaching to cause alerts, or if there are perceived unreasonable restrictions.
- Will take personal responsibility for professional development in this area.

3.6 **Students**

Students will:

- Adhere to the Acceptable Use Policy.
- Engage in age-appropriate online safety education opportunities.
- Respect the feelings and rights of others both on and offline.
- Take responsibility for keeping themselves and others safe online.
- Seek help from a trusted adult, if they have a concern related to their online activities and will support others that may be experiencing online safety issues.

3.7 **Families**

Families will:

- Read this policy and Acceptable Use appendices and encourage their children to adhere to it.
- Support the school in the implementation of this policy by discussing online safety issues with their children, and reinforcing safe online behaviours at home.
- Role model safe and appropriate use of technology and social media, and will endeavour to understand the ways in which they are using the internet, social media and their mobile devices to promote responsible behaviour.
- Endeavour to identify changes in their child's behaviour that could indicate that their child is at risk of harm online.
- Seek help and support from the school, or other appropriate agencies, if they or their child have online safety concerns.
- Use school systems, such as learning platforms and other network resources, safely and appropriately.
- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.

4. Potential harm to children and duty of care

4.1 We know that some adults and young people will use technology to harm others, particularly if they perceive a vulnerability. The breadth of issues associated with online safety is considerable but can be classified into 4 main areas of safeguarding risk:

Content: being exposed to illegal, inappropriate or harmful material for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.

Contact: being subjected to harmful online interaction with other users; for example: 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: online behaviour that increases the likelihood of, or causes harm; for example: 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.

Commerce: risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

4.2 As well as being used as a form of, or prelude to abuse, online communication can be used to intentionally polarise positions leading to young people feeling excluded or isolated. We are aware that young people often cite social media as a cause of anxiety. More recently, research has increasingly begun to explore the harmful effects of social media for example on body image and self-esteem, social isolation and depression. As such, social media may have a negative effect on young people's mental health.

4.3 There is a duty of care for all employees to educate the young people in our care on the risks and responsibilities associated with the use of technology and online safety. In all our academies, education on online safety happens in IT lessons, PSHE and assemblies. Sometimes other agencies such as the police may come in to support the programme of education. All education is age-appropriate and specific to the experience of the young person at a particular stage in their development. Teachers should never underestimate the importance of taking the opportunity to educate as the moment arises, for example a high-profile case.

4.4 This policy aims to be an aid in regulating activity and supporting the education of conduct online both inside and outside of academy hours. Online safety is a whole-school issue and is everyone's responsibility.

4.5 As well as protecting and educating young people, it is vital that they understand that actions have consequences and that inappropriate use of IT to harm others, will not be accepted. Every academy has a table of sanctions that relates to their specific approach to managing behaviour and reference is made to inappropriate use of IT. Students must be mindful that purposefully harming any member of our community or expressing views which could bring individuals or the organisation into disrepute, will not be tolerated.

5. Making use of IT to enhance learning and improve communication

5.1 The Internet and online platforms are used in all our academies to raise educational standards, to promote student achievement, to support the professional work of staff and to enhance communication. Members of staff will evaluate websites, tools and apps fully before use in the classroom or recommending for use at home. Support is available from the IT team.

5.2 Technology is advancing rapidly and is now a huge part of everyday life, education and business. We want to equip our students with all the necessary IT skills that they will need to enable them to progress their future careers confidently they leave The Two Counties Trust in a safe manner.

5.3 The Trust uses a wide range of technology. This includes:

- Computers, laptops, tablets and other digital devices.
- Internet which may include search engines and educational websites.
- School learning tools/portals.
- Email.
- Digital cameras, web cams and video cameras.

5.4 All school owned devices will be used in accordance with the requirements contained in the Acceptable Use appendices in this policy and with appropriate safety and security measures in place. All school devices are subject to school filtering and monitoring arrangements.

5.5 Schools will use age-appropriate search tools such as Google Safe Search.

5.6 Students will be appropriately supervised when using technology, according to their ability and understanding.

Some of the benefits of using IT including the internet are:

For students:

- Unlimited access to worldwide educational resources and institutions such as art galleries, museums and libraries.
- Access to subject experts, role models, inspirational people and organisations. The internet can provide a great opportunity for student.
- To interact with people that they otherwise would never be able to meet.
- An enhanced curriculum; interactive learning tools; collaboration, locally, nationally, and globally;
- Assessment: updates on current affairs as they happen.
- Access to learning whenever and wherever convenient.
- Freedom to be creative.
- Freedom to explore the world and its cultures from within a classroom.
- Social inclusion, in class and online.
- Access to case studies, videos and interactive media to enhance understanding.
- Individualised access to learning.

For staff:

- Professional development through access to national developments, educational materials and examples of effective curriculum practice and classroom strategies.
- Immediate professional and personal support through networks and associations.
- Improved access to technical support.
- Ability to provide immediate feedback to families.
- Class management, attendance records, schedule, and assignment tracking

6. Evaluating internet content

6.1 With so much information available online it is important that students learn how to critically evaluate information. Students will be taught to:

- Be critically aware of materials they read and shown how to validate information before accepting it as accurate.
- Use age-appropriate tools to search for information online.
- Acknowledge the source of information used and to respect copyright. Plagiarism is against the law and any intentional acts of plagiary are taken very seriously. Further action will be taken with students who are found to have plagiarised work. If they have plagiarised in an exam or a piece of coursework, they may be prohibited from completing that exam and /or the full series of examinations.

6.2 Academies have internet filters to ensure that content is appropriate to the age and maturity of students. If staff or students discover unsuitable sites, the URL will be reported to the Designated Safeguarding Lead in the school. Any material found by members of the school community that is believed to be unlawful will also be reported to the appropriate agencies. Regular checks will take place through IT to ensure that filtering services are working as expected.

Due to the global and connected nature of the Internet, it is not possible to guarantee with 100% certainty, despite systems in place that unsuitable or offensive material cannot be accessed via an academy computer or device and therefore vigilance is everyone's responsibility.

Users must not view, retrieve, download or share any offensive material. Offensive material includes, but is not limited to, content that is abusive, racist, considered to be of an extreme or terrorist related nature, sexist, homophobic, any form of bullying, pornographic, defamatory or criminal activity.

7. E-mail

7.1 The Trust uses email internally for staff and students and externally for contacting families and outside agencies, particularly in the case of potential safeguarding matters; it is an essential part of our communication and can often provide an important audit trail .

7.2 Staff and students must be aware that TTCT email accounts should only be used for work-related matters. The Trust has the right to monitor emails and their contents and in the case of a subject access request, emails will be produced and shared, unless there would be a specific safeguarding reason that would prohibit this.

7.3 **Staff should be aware of the following when using e-mail**

- Only use official TTCT email accounts to communicate with pupils and families. Personal email accounts should never be used to contact any of these people.
- Emails sent from a TTCT account should be professionally and carefully written. Staff are always representing the Trust and should take this into account when entering into any email communication.
- Remember that an e-mail is a written record.
- Never disclose confidential or personal information unless absolutely necessary, and where necessary ensure this is secured before sending, for example encrypted or password protected.
- Alert a member of IT to any suspicious e-mails, without forwarding them on or use the phishing button if you suspect a phishing e-mail.

7.4 **Students should be aware of the following when using e-mail**

Students will be taught to follow these guidelines through the IT curriculum and in any instance where e-mail is being used within the curriculum or in class:

- When in the academy they should only use approved email accounts.
- They must tell a member of staff if they receive any offensive, threatening or unsuitable emails either from within the academy or from an external account. They should not attempt to deal with this themselves.
- They must be careful not to reveal any personal information over e-mail or arrange to meet up with anyone who they have met online without specific permission from an adult in charge.
- Students will be educated to identify spam, phishing and virus e-mails and attachments that could cause harm to their wellbeing, school network or personal account.

8. Use of video conferencing technology

8.1 Online meeting invitation links must not be shared with, or accessed by others, unless permission has been granted by the meeting organiser.

8.2 The use of online learning tools and systems must be in line with privacy policies and data protection policies.

8.3 When delivering online lessons, the following must be followed:

- Normally, no 1:1 activity with pupils, groups only. When 1:1 contact is required, such as for wellbeing calls, careers interviews or post-16 tutorials, these calls may be made by a work telephone, in line with the Code of Conduct, or using Teams. Any 1:1 Teams calls must be recorded using the record function with the recording being retained by the teacher. Students cameras remain disabled.
- Staff must wear appropriate clothing, and anyone else in the household who may appear must be appropriately clothed.
- Any computers used should be in appropriate and accessible areas, for example, not in bedrooms; and the background should be blurred or the TTCT background added in Teams (staff).
- Students must have video cameras switched off.

- Live classes should be kept to a reasonable length of time.
- Language must be professional and appropriate, including anyone else present in the household who can be seen or heard in the background.
- Staff must only use platforms provided by the Trust to communicate with pupils and must not use their personal devices.
- Staff should record, the length, time, date and attendance of any sessions held.
- Staff must follow Trust guidance when setting up online lessons to ensure that appropriate safeguarding settings are in place to prevent unauthorised use and access to online lessons.

9. Social networking, use of IT, social media and personal publishing

9.1 Personal publishing tools include blogs, wikis, social networking sites, bulletin boards, chat rooms and instant messaging.

9.2 These online forums are the more obvious sources of inappropriate and harmful behaviour and where students are potentially more vulnerable to content, contact and conduct issues. It is important to educate students so that they can make their own informed decisions and take responsibility for their conduct online.

9.3 **Students**

Students are not allowed to access social media sites in any of our academies and we do not allow the use of mobile phones in our academies.

Social media sites have many benefits for both personal use and professional learning; however, both staff and students should be aware of how they present themselves online. Students are taught this through the IT curriculum and PSHE about the risks and responsibility of uploading personal information and the difficulty of taking it down completely once it is in the public domain. All our academies teach the following general rules on the use of social media and social networking:

- Students are educated on the dangers of social networking sites and how to use them in a safe manner. They are all made fully aware of the expected code of conduct regarding the use of IT and technologies and behaviour online.
- They are taught in age-appropriate way about the possible safeguarding dangers of online communication.
- Any sites that are to be used in class will be risk-assessed by the teacher in charge prior to the lesson to ensure that the site is age-appropriate and safe for use.
- The Trust's online filter (blocks inappropriate sites and searches in each academy and this is reviewed at least annually by the IT team.
- The Trust uses an online safeguarding system to monitor student searches and IT use to identify potential harmful online behaviour and to safeguard vulnerable students with flagged key words reported to the Designated Safeguarding Lead
- Students should not publish specific and detailed private thoughts, especially those that might be considered hurtful, harmful or defamatory.
- Students are warned against sharing or liking seemingly harmless messages which may have been shared by extremist organisations.
- The Trust expects all students to remember that they are always representing their academy and the Trust must act appropriately and in line with our ethos.

9.4 **Staff**

Not only do all staff have a duty of care towards young people, they are also duty-bound as professionals to use IT appropriately both within and beyond the organisation. In the same way as there can be consequences for young people, there can be for staff.

We ask staff to be mindful of their digital footprint and ensuring communication meets the 'red face test'. Our staff understand that any apparently private digital communication can become public and if it does, this could cause them, or the organisation, considerable embarrassment.

Safe and professional behaviour of staff online will be covered at staff induction. Appropriate conduct on social media is referenced in the Conduct of Conduct, Social Media Guidelines and also in Part Two of the Teachers' Standards. It is not expected that any employee will digitally communicate anything that could bring their profession, their academy or the Trust into disrepute.

Any views expressed on social media, e.g., Twitter, Facebook, Instagram, TikTok or LinkedIn for example, must make clear that they are the employee's own and must not lead to a reputational risk through association.

Staff must be aware that digital communication can be misunderstood and or misquoted and may lead to misunderstandings that could put them at risk of safeguarding allegation. For those who work with children or young people, Keeping Children Safe in Education makes clear that an allegation may be made against someone if they have 'behaved or may have behaved in a way that indicates they may not be suitable to work with children'. This includes online behaviour that may occur inside or outside of the place of work.

All staff will be provided with online safety updates as part of their routine safeguarding and child protection training including on specific safeguarding issues such as sharing nudes and semi-nude images and or videos, cyberbullying, radicalisation and dealing with harmful online challenges and online hoaxes. This includes being able to recognise the additional risk that children with Special Educational Needs and Disabilities (SEND) face online, so that staff are confident they have the capability to support SEND children to stay safe online.

As set out on the Code of Conduct, employees must never communicate with students on social media, by personal text or by any online platform other than those used legitimately in the academy and only ever in relation to learning.

Where safeguarding incidents involve youth produced sexual imagery, staff will not view, or forward sexual imagery reported to them and will follow the policy as set out in the Safeguarding and Child Protection Policy and procedures and relevant legislation and guidance.

The Headteacher will determine the level of information that will be provided to agency staff and volunteers, depending on their roles and requirements. All training will be providing as part of the academy's approach to safeguarding.

All staff are advised to safeguard themselves and their privacy when using social media sites. Advice will be provided to staff via training and by sharing appropriate guidance and resources. This will include (but is not limited to):

- Setting the privacy levels of their personal sites as high as possible.
- Being aware of location sharing services.
- Opting out of public listings on social networking sites.
- Logging out of accounts after use.
- Keeping passwords safe and confidential.
- Ensuring passwords are complex and are not shared.

Staff should not identify themselves as employees of the academy on their personal social networking accounts. This is to prevent information on these sites from being linked with the academy and also to safeguard the privacy of staff.

Information and content that staff have access to during the course of their employment, including photos and personal information about students and their family members or colleagues must not be shared or discussed with anyone else, including on any social media sites.

Staff will notify a member of the leadership team immediately if they consider that any content shared on social media sites conflicts with their role in the school.

10. Mobile telephones and personal devices

10.1 While mobile phones and personal communication devices are commonplace today, their use and the responsibility for using them should not be taken lightly. Some issues surrounding the possession of these devices are they can:

- Make students and staff more vulnerable to cyberbullying.
- Be used to access inappropriate internet material.

- Be a distraction in the classroom and the place of work.
- Are valuable items that could be stolen, damaged, or lost.
- Can have integrated cameras, which can lead to child protection, bullying and data protection issues.

10.2 The Trust does not permit student use of mobile phones in any of our academies. We discourage staff from using mobile phones other than for specific work purposes (e.g. early alert).

10.3 The Trust will not tolerate cyber bullying against either students or staff. Sending inappropriate, suggestive or abusive messages is forbidden and anyone who is found to have sent a message of such content will be disciplined. Information on the disciplinary sanctions for students set out in the behaviour policy.

10.4 A member of staff can confiscate mobile phones, and a member of the senior leadership team can search the device if there is reason to believe that there may be evidence of harmful or inappropriate use on the device.

10.5 Any student who brings a mobile phone or personal device into an academy agrees that they are responsible for its safety. The academy will not take responsibility for personal devices that have been lost, stolen, or damaged.

11. Mobile telephones and personal device misuse

11.1 **Students**

- Students who breach this policy in relation to the use of personal devices will be disciplined in line with the behaviour policy. Their mobile phone will be confiscated.
- Under no circumstances may a student bring a mobile phone or personal device into an examination room with them. If a student is found with a mobile phone in their possession it will be confiscated. The breach of rules will be reported to the appropriate examining body and may result in them prohibited from taking that exam or having their grades cancelled.

11.2 **Staff**

- Under no circumstances should staff give their personal telephone number or email address to families or students.
- Staff must have permission to take photos or videos of pupils and must not use their personal device at any time, only using academy supplied devices.
- The Trust expects staff to lead by example. Personal mobile phones should be switched off, out of view or on 'silent' whenever possible, unless they are being used for a specific work purpose.
- Any breach of the policy may result in disciplinary action. More information on can be found in the child protection and safeguarding policy, the disciplinary policy, dealing with allegations against members of staff policy and the contract of employment.

12. Cyber-bullying

12.1 As with any other form of bullying, cyber-bullying is taken very seriously. Information about specific strategies or programmes in place to prevent and tackle bullying is set out in the anti-bullying policy. The perceived anonymity that can come with using the internet can sometimes make people feel safe to say and do hurtful things that they otherwise would not do in person. It is made very clear to members of our community what is expected of them in terms of respecting their peers, members of the public and staff, and any intentional breach of this will result in further action.

12.2 If an allegation of cyber-bullying arises, the academy will:

- Take it seriously.
- Act as quickly as possible to establish the facts. It may be necessary to examine systems and user logs or contact the service provider to identify the cyber-bully.
- Record and report the incident.
- Provide support and reassurance to the victim.
- Make it clear to the cyber-bully that this behaviour will not be tolerated. If a group of people are involved, they will be spoken to individually and as a group. It is important that children who have harmed another,

either physically or emotionally, redress their actions and the academy will make sure that they understand what they have done and the impact of their actions.

12.3 If a sanction is used, it will correlate to the seriousness of the incident and the cyber-bully will be told why it is being used. They will be instructed to remove any harmful or inappropriate content that has been published. Repeated cyber-bullying may result in a suspension or if the behaviour is on-going and systematic, permanent exclusion may be considered.

13 . Upskirting

13.1 Upskirting typically involves taking a picture under a person's clothing without them knowing, with the intention of viewing parts of their body or clothing, not otherwise visible, to obtain sexual gratification, or cause the victim humiliation, distress or alarm.

13.2 Upskirting is a criminal offence. Attempting to commit an act of upskirting may also be a criminal offence e.g. if actions are taken to do something that is more than merely preparatory to committing the offence such as attempting to take a photograph on a telephone or camera but failing to do so because of lack of storage space or battery. The academy will treat incidences of upskirting as a breach of discipline and also as a safeguarding matter under the child protection procedures (see Safeguarding and Child Protection Policy and procedures).

13.3 If you are concerned that you have been a victim of upskirting, speak to a Trusted Adult or the Designated Safeguarding Lead as soon as possible.

14. Managing emerging technologies

14.1 Technology is progressing rapidly, and new technologies are emerging all the time.

14.2 The Head of IT will ensure that any new technologies are risk assessed before they are allowed into our academies and will consider any educational benefits that they might have. New technologies must not be adopted in academies without the approval of the Head of IT.

14.3 The Trust is conscious of the risks that new technology may attract, however, we also do not want to inhibit our students' learning by not allowing them access to the most up to date platforms.

15. Academy procedures

15.1 All students, staff and other adults have a responsibility to use the academy's computer system in a professional, lawful, and ethical manner. To ensure that all users are fully aware of their responsibilities when using technology, they are required to read and sign the appropriate Acceptable Use appendix.

15.2 In the event of an online safety incident involving illegal activity, the academy will:

- Inform the appropriate staff member as detailed below.
- Inform the Designated Safeguarding Lead.
- Inform the Headteacher.
- Inform the Head of IT.
- Inform the CEO for incidents involving the Headteacher.
- Secure and preserve all evidence and hardware.
- Report the incident to the appropriate agencies, such as: IWF, the Police or CEOP.
- Take internal action through the school's Behaviour, Anti-Bullying and Child Protection Policies, as appropriate.

15.3 Online safety incidents that involve inappropriate rather than illegal activity will be dealt with through the school's Behaviour, Anti-Bullying and Child Protection Policies, as appropriate.

15.4 Anyone who has any concern about the welfare and safety of a student must report it immediately to the Designated Safeguarding Lead in accordance with the Safeguarding and Child Protection Policy and procedures.

15.5 The academy reserves the right to withdraw access to the academy's IT network by any user at any time and to report suspected illegal activity to the police.

15.6 A log of all reported online safety incidents will be maintained by the academy's Designated Safeguarding Lead. Online safety incidents will also be reported to the Trust Designated Safeguarding Lead.

16. Delivering online lessons (See appendix 1)

16.1 We may on occasion deliver online lessons.

16.2 We recognise that synchronous (real-time video conferencing) poses more of a risk than asynchronous (e.g. setting work via a VLE), however, both deliveries need to be considered from a safeguarding perspective.

16.3 It is absolutely vital that clear protocols are adhered to in order to minimise potential safeguarding issues. Each academy must have a home-school agreement specifically related to online lessons (see below) which explains the role of the academy, the expectations of the student, and the expectations of the family.

16.4 All online lessons must be timetabled in the same way that physical lessons are and the Headteacher must know when lessons are occurring.

16.5 No change to the timetable should be made without agreement from a member of the academy SLT.

16.6 In the home-school agreement there should be reference to where lessons should take place and the importance of maintaining professionalism and an appropriate teacher-student relationship is maintained. There will be a clear expectation of conduct, as there is in the classroom, and also a dress code.

16.7 The online environment will be kept as formal as possible, and no informality of communication will be allowed to develop. Teachers need to be aware that online material can be published in a way in which it is not intended and remain vigilant to malicious publishing of videos that could bring the individual and the academy or Trust into disrepute.

16.8 No teacher will deliver online lessons without having received safeguarding and behaviour management training.

17. General Data Protection Regulation

17.1 All data within this policy will be processed in line with the requirements and protections set out in the General Data Protection Regulation.

Appendix 1. Remote learning safeguarding guidance

1. Introduction

1.1 The Two Counties Trust is committed to providing students with a safe learning experience, whether conducted face to face or remotely. The safeguarding of the young people in our care is paramount.

1.2 The opportunity to use new technologies to either enhance or replace face to face learning is one that it is vital for us to take. We believe that through embracing new technologies we can remove the barriers faced by students as a result of enforced school closures, long term illness or unavoidable absence.

1.3 We recognise that online learning may present particular safeguarding risks that may not all be present in a physical classroom. With clear protocols and high expectations of conduct, we believe we can minimise, if not eliminate, potential issues.

1.4 It is important that all staff and teachers who interact with children and young people, including online, continue to look out for signs that a young person may be at risk. Any such concerns should be dealt with in line with the Safeguarding and Child Protection Policy.

1.5 The usual safeguarding procedures for reporting issues will remain in place with teachers and staff able to raise concerns to the Designated Safeguarding Lead.

1.6 This guidance is in place to protect all students and staff.

2. Overview

2.1 The Two Counties Trust is committed to providing the highest standard of safeguarding. The safety of our young people is of paramount concern.

2.2 The Two Counties Trust is working towards only using Microsoft Teams as its online learning platform for the delivery of both synchronous (real time) and asynchronous (pre-prepared and or recorded) lessons.

2.3 All synchronous lessons will be timetabled, and the times will be published on the academy website. No changes to lesson times will take place without the permission of the Headteacher.

2.4 Before the academy undertakes synchronous lessons, families will have the opportunity to ask questions and withdraw their consent from involvement if they do not feel satisfied with the measures that are in place.

3. Legislation

3.1 Our policies and procedures have been developed to ensure we comply with all relevant safeguarding legislation and in particular the statutory guidance, Keeping Children Safe in Education.

4. Aims of the guidance

4.1 The Two Counties Trust seeks to provide the best possible safe learning environment.

4.2 This guidance aims to ensure we safeguard all users of The Two Counties Trust online learning (including children, families, and staff).

4.3 All teachers who deliver online learning will be trained in safeguarding and will be familiar with this guidance, the Safeguarding and Child Protection Policy and Keeping Children Safe in Education.

4.4 If any family has a safeguarding concern about a member of staff, they must contact the Headteacher of the academy immediately who will manage the concern in accordance with established procedures.

5. Responsibilities

5.1 All staff receive regular safeguarding training. They fully understand the duty to safeguard young people and what to do in the event of an incident.

5.2 Synchronous online lessons will be quality assured in real-time, in the same way that classroom learning is, by drop-ins; a senior member of staff is on duty at all times during online lessons.

5.3 All data will be protected in accordance with relevant legislation and Data Protection policies.

5.4 The senior leadership team and the Designated Safeguarding Lead are able to monitor postings made on Teams and messages sent between students and teachers.

5.5 Online lessons will be recorded (aside from normal timetabled lessons students dial into or where any unforeseen malfunction of the recording equipment occurs) and store these recordings for a minimum of 30 days and a maximum of 90 days. These recordings remain the property of the Trust.

5.6 The Trust will ensure all complaints are dealt with in line with the Complaints Procedure

5.7 The academy will train teachers on online transparency before they deliver online lessons, , for example, ensuring student and teacher hands are folded and in view at all times, not turning off screens (only speakers), ensuring student engagement through techniques such as using the chat facility, and directing questions.

5.8 The Trust will regularly review this guidance to ensure it is best suited to safeguarding all users.

6. Student responsibilities

6.1 Students under the age of 18 must have consent from a family member for them to receive online synchronous learning.

6.2 Students have a personal responsibility to ensure that there is no inappropriate communication between themselves, other students and the teacher.

6.3 If a student believes that any communication has been inappropriate, they must do what they would do in a lesson in the academy and report this to their Head of Year, their trusted adult, the Designated Safeguarding Lead or a member of SLT immediately.

6.4 If there is anything that makes a student feel uncomfortable about the content or delivery of the lesson, they must report this to their Head of Year, their trusted adult, the Designated Safeguarding Lead or a member of SLT immediately.

6.5 Students are solely responsible for the material they post online, including messages sent, and they must not post defamatory, offensive or illegal material.

6.6 Students must report to any defamatory, offensive or illegal material they view on our platform to their Head of Year, their trusted adult, the Designated Safeguarding Lead or a member of SLT immediately.

6.7 Young people should expect the same standard of behaviour in online lessons as there would be in a lesson in the academy and the same behaviour management system will be applied. They must wear their school uniform as they would in the academy.

6.8 Students must ensure that staff are treated with respect.

6.9 Students must report any safeguarding concerns or illegal activity immediately to their parent, their Head of Year, their trusted adult the Designated Safeguarding Lead or a member of SLT immediately.

6.10 Students must undertake an online lesson in an appropriate place where there is the potential for an adult to supervise. They must not be in a bedroom so that professionalism is maintained. Siblings should not interrupt learning.

6.11 Students must confirm that they understand the importance of using all materials as they are intended and that any attempt to misuse or misrepresent the teacher or the academy will be taken extremely seriously. If other students become aware of this happening, it is expected that they will report this immediately.

6.12 For synchronous live lessons that are a part of student's normal daily timetable, headphones should be worn. This is also necessary to protect the data of other students in the classroom.

7. Teacher responsibilities

7.1 If a lesson is arranged and timetabled, it will go ahead in the same way that it would in the academy, even if this is with a cover teacher. Parents will always know the timetable for online synchronous lessons.

7.2 Teachers are responsible for the learning that takes place online and are monitored and held to account for the quality of planning and delivery in the same way that they are in the academy classroom.

7.3 Teachers must immediately report any defamatory, offensive, or illegal material they view on our platform.

7.4 Should the teacher notice that there is an issue with recording the lesson, either human error or technical, they should explain to the students that the lesson must be terminated and immediately inform the Headteacher and the Designated Safeguarding Lead. The lesson will then be formally rearranged. If the teacher realises at the end of the lesson that it has not been recorded, they must immediately inform the Headteacher and Designated Safeguarding Lead and report any issues.

7.5 Teachers must manage behaviour in the same way that they would in the physical classroom.

7.6 If a student continues to disrupt a lesson, the teacher should call for 'on call' in the same way that they would in a lesson in the academy. A student will not be removed from a lesson with no supervision without a parent being informed. A student who is being disruptive will be muted until on call is able to attend. The academy will ring the parent immediately to explain the issue and then follow up.

7.7 Teachers must take every precaution to ensure that they work in a safe and professional environment and that all lessons are delivered in an open and neutral space, where possible in the presence of another teacher, either physically or online.

7.8 Teachers must ensure that their environment does not display any inappropriate images or documents when conducting a session and that, if the lesson is delivered remotely, that the TTCT background is used

7.9 Teachers must follow the Code of Conduct at all times and the Teachers' Standards.

7.10 Where a difficulty arises with a student's conduct, the parent will be involved in the same way that they would be in the academy.

7.11 At the start of online learning, the teacher will make clear the expected conduct and the sanctions that will be applied.

7.11 Teachers must report any behavioural issue in the same way that they usually would.

7.12 Any safeguarding concerns or illegal activity must be reported immediately to the Designated Safeguarding Lead.

7.13 Teachers must ensure that, if anything, online lessons are more formal than in a classroom setting and that they do not make any comments which could be misconstrued or misinterpreted.

7.14 The platform must be used for formal lesson delivery and for no other purpose. All conversations should be learning related and never with just one student unless there is adequate supervision.

7.15 The teacher must ensure that they record the lesson from the minute that they enter the 'room' and that they are present before any students.

8. Family responsibilities

8.1 The family will be responsible for the welfare of the student during the session.

8.2 The family will always be responsible for the student's physical environment during the session and will ensure it is safe and appropriate.

8.3 If possible, the parent or another responsible adult will be present for secondary school students, or available, during an online lesson so that any concerns encountered by the student can be reported as soon as possible.

8.4 The family will work with the academy to ensure the student adheres to the behavioural expectations and is meeting the terms of their home-academy contract. Any misuse of online learning materials, for example for malicious purposes, will be treated extremely seriously. If a teacher or the academy's reputation is damaged as a result, the sanction could be permanent exclusion.

8.5 The family will raise any concerns regarding the quality of learning with the Head of Year or a senior leader.

8.6 The family will support the organisation of the student, making sure they are equipped and ready to learn and that all independent home learning is completed on time and is of best quality.

8.7 Any safeguarding concern will be reported immediately to the designated safeguarding lead.

Appendix 2. Acceptable Use Policies

Staff Acceptable Use Policy

1. Introduction

- IT and related technologies such as e-mail, the Internet and mobile devices are an expected part of our daily working life.
- This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of IT.
- All staff must always adhere to this policy.
- Staff should be aware that a breach of this acceptable use policy may result in disciplinary proceedings.

2. Expectations of staff

- To only use work e-mail and any related technologies for professional purposes.
- To limit internet for personal use to out of working time and to breaks and lunchtime.
- To comply with the IT system security.
- To keep passwords secure.
- To ensure that personal details cannot be accessed by those not authorised to have them.
- All electronic communications with pupils and staff are compatible with professional responsibilities.
- Personal details, such as mobile phone number and personal email address must not be disclosed to students or families.
- All personal data is to be kept secure and used appropriately, whether on or off the premises.
- No hardware or software will be installed without the permission of the IT Department.
- Any material that could be considered offensive, illegal or discriminatory will not be browsed for, downloaded, uploaded or distributed.
- Personal devices must not be used to record images of students and images of students must not be downloaded to personal devices.
- To accept that use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to the Headteacher and / or a member of the Trust's Executive Team.
- To adhere to e-safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the Trust community.
- To respect copyright and intellectual property rights.
- All online activity, both in Trust and outside Trust, will not bring the professional role for which staff are employed into disrepute.
- Not to permit any current pupil of any age or any ex-pupil of the Trust under the age of 21 as a friend, follower, subscriber or similar on any personal social media account, including any form of online gaming.
- To only use sanctioned social media accounts for communicating official Trust business or news and in accordance with established procedures.

Signed:

Date:

Print name:

Visitor/Volunteer Acceptable Use Policy

As a professional organisation with responsibility for safeguarding it is important that all members of the school community are fully aware of their professional responsibilities and read and sign this Acceptable Use Policy.

This is not an exhaustive list; all members of the academy community are reminded that IT use should be consistent with the academy ethos, policies, national/local guidance and expectations, and the law.

All references to school include the academy and The Two Counties Trust.

- I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with The Data Protection Act and the Data Protection Policy. Data will not be removed from site. Any images or videos of pupils will only be used as stated in the online safety policy and will always take into account parental consent and will never be taken by or stored on personal devices.
- I have read and understood the online safety policy which covers the requirements for safe IT use, including using appropriate devices, safe use of social media websites and the supervision of students within the classroom and other working spaces.
- I will follow the policies regarding confidentially, data protection and use of images and will abide with copyright and intellectual property rights, child protection legislation, privacy and data protection law and other relevant civil and criminal legislation.
- I will respect system security and I will not disclose any password or security information that is given to me. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate.
- My electronic communications with pupils, families and other professionals will only take place within clear and explicit professional boundaries and will be transparent and open to scrutiny at all times.
- All communication will take place via approved communication channels such as via a school provided email address or telephone number and not via personal devices or communication channels such as via personal email, social networking sites or mobile phones.
- My use of IT and information systems will be compatible with my role within school. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites. I will take appropriate steps to protect myself online and my use of IT will not interfere with my work duties and will always be in accordance with this Acceptable Use Policy and the law.
- I will not create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role, the academy, into disrepute.
- I will promote online safety with the children in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.
- If I have any queries or questions regarding safe and professional practice online either in school or off site, I will raise them with the Designated Safeguarding Lead.
- I will report any incidents of concern regarding online safety to the Designated Safeguarding Lead as soon as possible.
- I understand that if the academy believes inappropriate use or unacceptable behaviour is taking place, the academy may refuse me any further access. If the academy suspects criminal offences have occurred, the matter will be brought to the attention of the relevant law enforcement organisation.

Signed:

Date:

Print name:

Student Acceptable Use Policy (KS3/4/5)

1. Introduction

This acceptable use policy is intended to ensure:

- That young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- That academy systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

The academy aims to ensure that students will have good access to digital technologies to enhance their learning and will, in return, expect students to agree to be responsible users.

2. Expectations of students:

I understand that I must use the academy IT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the IT systems and other users.

For my own personal safety:

- I understand that the academy will monitor my use of IT systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may see it or steal it.
- I will be aware of "stranger danger" when I am communicating online.
- I will not disclose or share personal information about myself or others when online (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details, etc.)
- I will not arrange to meet people off-line that I have communicated with online.
- I will immediately report to a member of staff any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it online.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the academy systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the academy systems or devices for online gaming, online gambling, internet shopping. I will only use academy systems or devices for file sharing, or video broadcasting (eg YouTube), when I have permission of a member of staff to do so.

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.
- When participating in online lessons, I will uphold the responsibilities expected of me which are set out in the Remote Learning Safeguarding Guidance.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the academy:

- I will only use my own personal devices (mobile phones / USB devices etc) in school if I have permission I understand that, if I do use my own devices in the academy, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.

- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software; however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person / organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.
- I will only use social media sites with permission and at the times that are allowed.

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the academy also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the academy community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy, I may be subject to disciplinary action. This may include loss of access to the academy network / internet, correction, suspensions, contact with parents, and in the event of illegal activities involvement of the police.

Please complete the sections on the next page to show that you have read, understood and agree to the rules included in the Acceptable Use Policy. If you do not sign and return this agreement, access will not be granted to IT systems and devices.

Wi-Fi Acceptable Use Policy (Guest and BYOD Access)

As a professional organisation with responsibility for safeguarding it is important all members of the school community are fully aware of the boundaries and requirements when using the academy Wi-Fi systems, and take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft.

This is not an exhaustive list; all members of the academy community are reminded that IT use should be consistent with the the academy ethos, policies, national/local guidance and expectations, and the law.

All references to School include the academy and The Two Counties Trust.

- The academy provides Wi-Fi for the academy community and allows temporary guest access for visitors and BYOD (Bring your own device) access for staff and sixth form pupils.
- I am aware that the academy will not be liable for any damages or claims of any kind arising from the use of the wireless service. The academy takes no responsibility for the security, safety, theft, insurance and ownership of any device used within the school premises that is not the property of the academy or is not part of a pupil 1 to 1 device scheme.
- The use of IT devices falls under the academy Acceptable Use Policy and the Online Safety Policy which all pupils, staff and other adults must agree to, and comply with.
- The academy reserves the right to limit the bandwidth of the wireless service, as necessary, to ensure network reliability and fair sharing of network resources for all users.
- School-owned information systems, including Wi-Fi, must be used lawfully and I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.
- I will take all practical steps necessary to make sure that any equipment connected to the academy's service is adequately secure, such as ensuring that connected equipment has up-to-date anti-virus software and system updates.
- Use of the academy's wireless service is done at my own risk. By using this service, I acknowledge that security errors and hacking are an inherent risk associated with any wireless network. For that reason, I expressly agree that I knowingly assume such risk, and further agree to hold the school harmless from any claim or loss arising out of, or related to, any such instance of hacking or other unauthorised use or access into my computer or device.
- The academy accepts no responsibility for any software downloaded and/or installed, e-mail opened, or sites accessed via the academy's wireless service's connection to the internet. Any damage done to equipment for any reason including, but not limited to, viruses, identity theft, spyware, plug-ins or other internet-borne programs is my sole responsibility; and I indemnify and hold harmless the school from any such damage.
- The academy accepts no responsibility regarding the ability of equipment, owned by myself, to connect to the wireless service.
- I will respect system security and I will not disclose any password or security information that is given to me. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate.
- I will not attempt to bypass any of the academy security and filtering systems or download any unauthorised software or applications.
- My use of the academy Wi-Fi will be safe and responsible and will always be in accordance with this Acceptable Use Policy and the law including copyright and intellectual property rights. This includes the use of email, text, social media, social networking, web publications and any other devices or websites.
- I will not upload, download, access or forward any material which is illegal or inappropriate or may cause harm, distress or offence to any other person, or anything which could bring the school into disrepute.
- I will report any online safety concerns, filtering breaches or receipt of inappropriate materials to the school's Designated Safeguarding Lead or IT Support as soon as possible.
- If I have any queries or questions regarding safe behaviour online then I will discuss them with the Designated Safeguarding Lead

- I understand that my use of the academy's Wi-Fi will be monitored and recorded to ensure policy compliance in accordance with privacy and data protection legislation. If the academy suspects that unauthorised and/or inappropriate use or unacceptable or inappropriate behaviour may be taking place, then the academy may terminate or restrict usage. If the academy suspects that the system may be being used for criminal purposes, the matter will be brought to the attention of the relevant law enforcement organisation.

Appendix 3: Filtering and Monitoring

1.Introduction

1.1 As is evident in this policy, The Two Counties Trust and its academies are committed to providing a safe environment to learn and work, including when online. Filtering and monitoring are important parts of safeguarding students and staff from potentially harmful and inappropriate online material.

2. Roles and Responsibilities

2.1 It is everybody's responsibility to ensure filtering and monitoring is effective. This includes the Safeguarding Trustee, a designated member of the Trust's Executive team, the Head of IT, the IT Support team, all staff as well as students. For specific responsibilities please refer to section 3 of the main policy.

3. Regular Review of Provision

3.1 Our filtering and monitoring systems automatically update to block unsuitable keyboards and websites. However, to proactively ensure our filtering and monitoring remains effective and meets the needs of students and staff, particularly when there is a change to technology or a safeguarding risk is identified, we review manually created policies which either allow or block content and other settings regularly, but with a full review of the whole system at least annually.

3.2 This review will take into account:

- The risk profile of our students, including their age, pupils with Special Educational Needs and Disability (SEND) and students with English as an Additional Language (EAL).
- What our filtering system currently blocks or allows and why.
- Any outside safeguarding influences such as County Lines.
- Any relevant safeguarding reports.
- The digital resilience of our students
- Teaching requirements for example the RSE and PSHE curriculum
- Related safeguarding and technology policies in place
- What checks are currently taking place and how resulting actions are handled.

This review will inform us in:

- Related safeguarding or technology policies and procedures.
- Roles and responsibilities.
- Staff training.
- Curriculum and learning opportunities.
- Procurement decisions.
- How often and what is checked.
- Monitoring strategies.

This review, and subsequent action, will be logged and kept on record using the form below.

Filtering and Monitoring Review Record

Date of check:	
Carried out by:	

Question	Fully in place	Partial/ Needs Review	Not in place	• Evidence / details and dates • Any actions / by whom? • Check items to add to risk register
Filtering				
Appropriate filtering Has your provider filed a submission with the UK Safer Internet Centre to explain why your filtering is 'appropriate'? Have DSL, SLT and technical teams all read and understood this submission, including rationale, benefits and limitations and safe search settings, e.g. for web searches and YouTube?				Safer Internet Centre submissions - https://saferinternet.org.uk/guide-and-resource/teachers-and-school-staff/appropriate-filtering-and-monitoring/filtering-provider-responses YouTube guidance - https://youtube.lgfl.net
Filtering training Has your technical team attended training on your filtering platform/s to understand exactly how it works, how it is set up and what the options are in order to inform a strategic filtering approach and implement DSL/SLT requirements? Has your safeguarding team also attended training to know the questions they need to ask of their technical colleagues and to understand at a high level what filtering can/should do to inform the approach?				Tech training - https://lgfl.bookinglive.com/book/add/p/23 Safeguarding training (20 minute overview) - https://lgfl.bookinglive.com/book/add/p/5
Rationale / team effort Do your technical and safeguarding teams meet to discuss your filtering needs and document your approach regarding what is allowed / not in school and the safeguarding-driven rationale? Is this up to date, reflected accurately (and updated) in policies and practice, including how your approach and settings do not 'over-block', and shared with parents, staff and governors and ready to show to Ofsted?				

Reporting and regular review Do you receive regular automated reports to inform safeguarding / behaviour interventions and review use of the system to keep users safe and ensure you are not over blocking (also important to ensure access to teaching & learning sites)? Who is responsible for checking these reports have been run and are being reviewed, and that they are functioning correctly? Is the system regularly reviewed to ensure appropriate access, settings and usage, including consideration of impact				e.g. Viewing top blocked sites / categories monthly will highlight trends and changes that need to be investigated or addressed by talking to students.
Safe modes / search Do you enforce safe search on search engines and block those which do not have a safe search? For YouTube, do you enforce one of the restricted modes as appropriate for your needs?				YouTube mode checked via https://youtubemode.lgfl.net YouTube settings overview at https://youtube.lgfl.net Check at the top right of the search page if Google safe search is enforced (LGfL schools request this via a DNS change)
BYOD If you allow 'bring your own device', what measures are applied to these devices to ensure the school internet cannot be used inappropriately simply by switching to a BYOD network				NB there are many different approaches – some schools do not allow BYOD; many do or restrict it to certain groups. Some schools insist upon logging in if using the BYOD network; others where this is not possible might choose to make it much more restrictive
Devices at home Have you applied filtering to school devices when sent home with students? Given that schools cannot protect parent/child devices, do you remind parents about how to set controls on their home internet/phones/devices etc?				Web filtering for school devices at home is available from various providers including LGfL – those solutions which also have Chrome extensions can also protect children if they access a school profile on a family device See https://parentsafe.lgfl.net for support with parental control settings and other ways parents can keep their children safe online
Linked to the curriculum and safeguarding landscape				An example for Q2 in this row – if there is a spike in failed attempts to view pornographic sites, is this covered in class as a priority, regardless of

Is your filtering set up and updated to reflect the online-safety messages you teach and safeguarding concerns/cases in school? Conversely, is learning from filtering findings used to inform the curriculum?				where it may fall in the scheme of work / plan for the year?
Monitoring				
Approach Is your approach to monitoring based on a strategic and safeguarding-driven rationale that has been made in discussion between safeguarding and technical teams? Are all senior leaders, governors and staff aware of this rationale and which of the three possible approaches (or combination) outlined by the Safer Internet Centre that your school follows.				Safer Internet Centre monitoring approaches - https://saferinternet.org.uk/guide-and-resource/teachers-and-school-staff/appropriate-filtering-and-monitoring/appropriate-monitoring
Appropriate monitoring If you use a pro/active technical monitoring solution, has the provider filed a submission to the UK Safer Internet Centre? Have DSL, SLT and technical teams all read and understood this submission, including rationale, benefits and limitations.				Safer Internet Centre appropriate monitoring provider submissions – https://saferinternet.org.uk/guide-and-resource/teachers-and-school-staff/appropriate-filtering-and-monitoring/monitoring-providers-responses
Monitoring training If using a pro/active solution, has your technical team attended training to understand exactly how it works, how it is set up and what the options are in order to inform a strategic approach and implement DSL/SLT requirements? Has your safeguarding team attended training to know the questions they need to ask of their technical colleagues and to understand at a high level what monitoring can/should do to inform the approach?				
System configuration, customisation and review Do your technical and safeguarding teams meet to discuss your monitoring needs and ensure systems are configured for the devices and systems you used and regularly updated/reviewed where changes are made and new devices added to ensure no devices or systems are missed?				

Are systems customised for your safeguarding needs – e.g. adding keywords that represent new concerns in your school/area or to follow students at particular risk. Is this approach documented and the system regularly reviewed to ensure appropriate access, settings and usage / do your policies reflect practice in school and are they updated when settings / approach are changed?				
Reports If using a pro/active solution, is the system set up in such a way that you have a manageable number of captures and are not overwhelmed and therefore at risk of missing key safeguarding alerts? Do you also run reports to spot trends over time? Are concerns fed into the safeguarding systems you use to capture manual/offline safeguarding concerns to complete the safeguarding jigsaw and not kept in a separate silo?				
Other Consider the school devices when at-home / curriculum / BYOD questions mentioned in the filtering section above and add any aspects not already covered there.				