The Learners Collective – Online Safety Policy

Statement Authorised By: Managing Director Designated Safeguarding Lead:	 Mr Rory Gaskin Mr Owais Yasin
Reviewed on:	05/09/2023
Next Review Due:	05/09/2024

The Learners Collective ("TLC") recognises its commitment to the safety of students, children and young people who engage with TLC and its tutors. This policy forms part of TLC's Safeguarding Policy and Procedures. Any issues and concerns with online safety must follow TLC's Safeguarding Policy and Procedures.

Introduction

The purpose of this policy is to:

- Ensure that the safety and wellbeing of students, children and young people is paramount when adults, young people or children are using the internet, social media or mobile devices.
- Set out the key principles expected of all Staff with respect to the use of IT-based technologies.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet during TLC sessions.
- Assist staff working with children to work safely and responsibly with the Internet and other IT and communication technologies.
- Provide TLC staff and tutors with the overarching principles that guide our approach to online safety.
- Ensure that all members of the TLC community are aware that unlawful or unsafe behaviour is unacceptable.
- Ensure that, as an organisation, we operate in line with our values and within the bounds of the law in terms of how we use online devices.
- Minimise the risk of misplaced or malicious allegations made against adults who work with students.

This policy applies to all TLC staff, tutors, children and young people and anyone involved in TLC's activities.

The Four Key Categories of Risk

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

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

- **Contact** – being subjected to harmful online interaction with other users, such as child-to-child pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes

- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and

- **Commerce** - risks such as online gambling, inappropriate advertising, phishing and any other financial scam.

Legal Framework

This policy has been created on the basis of legislation, policy, guidance and best practice that seeks to protect students, children and young people in the UK. Summaries of the key legislation and guidance are available on:

- Online Abuse
- Bullying
- Child Protection

It has also been based on the Department for Education (DFE)'s 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-bulling: advice for headteachers and school staff

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.

Role and Responsibilities

Senior Leadership Team

The Senior Leadership Team has overall responsibility for monitoring this policy, ensuring that staff understand this policy, and that it is being implemented consistently throughout the organisation.

The Senior Leadership Team will coordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The member of the Senior Leadership Team who oversees online safety is the DSL.

The Senior Leadership Team and the DSL are responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout.

All Senior Leadership Team members will:

- Ensure that they have read and understood this policy
- Agree and adhere to the terms on acceptable use of the organisation's Teaching Platform and Microsoft Teams (*Appendix 2*)
- Ensure that, where necessary, guidance for students around online safety awareness, is adapted for vulnerable children, victims of abuse and pupils with SEND 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.

The Designated Safeguarding Lead

Details of the organisation's DSL (Owais Yasmin) are set out in our Child Protection and Safeguarding Policy as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in the organisation, in particular:

- Refer safeguarding concerns involving the internet or online services to the local authority children's social care as required and support staff who make referrals to local authority children's social care
- Refer safeguarding concerns involving the internet or online services to the local authority children's social care as required and support staff who make referrals to local authority children's social care;
- Act as a point of contact with schools and colleges and their three safeguarding partners
- Confirm to schools and colleges that all processes and procedures with regard to online safety are in place and adhered to;
- Liaise with schools and colleges on matters of online safety and when deciding whether to make a referral to relevant agencies;
- Act as a source of support, advice and expertise for all staff on online safety. ● understand the lasting impact that adversity and trauma experienced online can have, including on children's behaviour, mental health and wellbeing, and what is needed in responding to this in promoting educational outcomes;
- Ensure each member of staff has access to, and understands, the company's online safety policy and procedures, especially new and part time staff;
- Understand relevant data protection legislation and regulations, especially the Data Protection Act 2018 and the General Data Protection Regulations;

- Are able to understand the unique risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online in education;
- Can recognise the additional risks that children with SEN and disabilities (SEND) face online, for example, from bullying, grooming and radicalisation and are confident they have the capability to support SEND children to stay safe online;
- Ensure the online safety policy is reviewed annually (as a minimum) and the procedures and implementation are updated and reviewed regularly;
- Ensure the online safety policy is available publicly and parents are aware of the fact that referrals about suspected abuse or neglect may be made and the role of the company in this.

This list is not intended to be exhaustive.

The Technology Lead

The Technology Lead is responsible for:

- Checking that there is an appropriate level of security protection procedures, such as monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure students are kept safe from potentially harmful and inappropriate content and contact online while with TLC, including terrorist and extremist material.
- Ensuring that the organisation's IT systems are secure and protected against viruses and malware, such as through the use of firewalls, antivirus and encryption, and that such safety mechanisms are updated regularly.
- Ensuring security measures, such as the monitoring of the organisation's IT systems, are implemented to the fullest extent possible on a regular basis
- Ensuring that the systems keep traceable records of any reported online safety incidents (see *Appendix 4*) available to the DSL when the incident is reported
- Ensuring that the systems are set up to allow lesson recordings so that any incidents or concerns recorded are made available to the DSL when reported

This list is not intended to be exhaustive.

All Staff

All staff and anyone who works for TLC are responsible for:

- Maintaining an understanding of this policy.
- Implementing this policy consistently.
- Agreeing and adhering to the terms on acceptable use of the organisation's Teaching Platform(s) and Zoom classrooms (see *Appendix 3*).
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the organisation's behaviour policy and reported to the DSL

- 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.

Parents and Carers

Parents and carers are expected to:

- Notify a member of staff or the Senior Leadership Team of any concerns or queries regarding this policy.
- Ensure their child has read, understood and agreed to the terms on acceptable use of the organisation's Teaching Platform and Microsoft Teams (Appendix 1 and 2)

Educating students about online safety

We ask all students to read and agree to our acceptable use agreements to ensure they have an awareness and understanding of online safety during online classes and when using TLC's Teaching Platform(s) and Microsoft Teams. Teams is a secure platform that we use to deliver our classes. Our teaching platform, TutorCruncher, includes an online safety guide for students.

The safe use of social media and the internet will be covered in classes, where relevant.

The safe use of social media and the internet will be covered in classes, where relevant. Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

Educating parents/carers about online safety

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

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

Cyber-bullying

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 by another person or group, where the relationship involves an imbalance of power. (See also the organisation's behaviour policy.)

Preventing and addressing cyber-bullying

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

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

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

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with the schools and/or local authorities and external services if it is deemed necessary to do so.

Acceptable Use

All students, parents, and tutors are expected to sign an agreement regarding the acceptable use of the organisation's Teaching Platform(s) (see *Appendix 1 and 2*).

Use of the organisation's Microsoft Teams classrooms must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will record all lessons and save all content posted in the chat of the organisation's Teams classrooms for safeguarding purposes, and to ensure students, parents and tutors comply with the above. These are stored securely in line with data protection legislation. More information is set out in our Data Protection Policy, Records Management, Retention and Disposal policy and acceptable use agreements.

Students using mobile devices in classes

Students are asked not to use their mobile devices at any time during classes, with the exception of instances where tutors give permission for students to use them for teaching and learning purposes (appendix 2) or to call for help in an emergency.

Any breach of the acceptable use agreement by a student may trigger sanctions in line with the organisation's behaviour policy.

Students, tutors and parents are not permitted to take photos of tutors or other students using mobile devices during online classes (appendix 2 and 3).

Staff using personal devices

Tutors using personal devices for teaching

Where tutors use personal devices for delivery of lessons and associated actions (e.g. marking homework), they must never store information containing personal data (e.g. a piece of homework with a student's name written on it) on the device. If homework, reports or similar documents need to be downloaded for the purposes of marking or filling in, they must be handled and deleted within the same session and never left on an unattended/unlocked computer. Actions that can be completed within TLC's online learning platforms (e.g. TutorCruncher) should be completed directly in the platform without storing information elsewhere (e.g. writing reports).

They must also ensure that others do not have access to their devices in ways that would enable them to view/make use of personal data and/or the teaching platform(s) of TLC. Steps to ensure this include but are not limited to:

- Setting up a separate user account on the device to ensure that other users of the equipment cannot access our teaching platform(s), on purpose or inadvertently
- Only accessing/transferring TLC-related data when using a secure (private) internet connection
- Using their dedicated TLC email address for all correspondence relating to their work for TLC
- Installing anti-virus and anti-spyware software and keeping these up-to-date
- Keeping operating systems up to date – always install the latest updates
- Ensuring the device is 'clean' and does not contain any inappropriate content that may be visible when screen sharing
- Tutors must comply with our data protection policy and procedures to ensure the safe and secure retention of students' personal data

How the organisation will respond to issues of misuse

Where a student misuses the organisation's Teaching Platform(s) or Microsoft Teams classrooms. We will follow the procedures set out in our policies on behaviour and acceptable use. Students that misuse these services will be reported to their school parents/guardians/carers or other appropriate agencies. Students may also be removed or banned from the course or programme.

Where a tutor misuses the organisation's Teaching Platform(s) or Microsoft Teams classrooms, the matter will be dealt with in accordance with the staff disciplinary procedures and staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The organisation will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police or children's social care in line with our safeguarding policy (where appropriate).

Training

All new tutors and staff 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 employees/workers 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).

By way of this training, all employees/workers 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 other children online through:
    - Abusive, harassing and misogynistic messages
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around group chats
    - Sharing of abusive images and pornography to those who do not want to receive such content
- Physical abuse, sexual violence and initiation/hazing type can all contain an online element

The training will also help staff:

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

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

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

Filtering and Monitoring

Governing bodies and proprietors should be doing all that they reasonable can to limit children's exposure to the above risks from various IT systems. As part of this process, the Senior Leadership Team will ensure that there are appropriate filters and monitoring in place. See Appendix 6 for the roles and responsibilities in relation to filters and monitoring.

Whilst considering their responsibility to safeguard and promote the welfare of children provide them with a safe environment in which to learn, TLC will consider the age range of their students, the number of students, how often they access the IT system and the proportionality of costs vs. risks.

The UK Safer Internet Centre has published guidance as to what "appropriate" might look like. Appropriate filtering and monitoring guidance on e-security is available from the National Education Network-NEN.

Use of Mobile Technology

Many children have unlimited and unrestricted access to the internet and TLC will carefully consider how this is managed whilst working with a commissioned student.

Whilst it is essential that we ensure that appropriate filters and monitoring systems are in place, they should be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding.

It is generally suggested, that due to the intensive nature of our delivery models, and the nature of the students we are commissioned to work with, students will not be allowed unsupervised access to ICT or mobile technology whilst on commission with TLC.

TLC works with external partners to review data and information security which incorporates online safety during intervention work. Government guidance around filtering and monitoring provides information for schools and colleges: https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/filtering-and-monitoring-standards-for-schools-and-colleges.

Where devices are owned and managed by TLC, we ensure that software is updated regularly, age-appropriate filters are in place and also known websites that may look to exploit vulnerable young people to engage in abusive or extremist behaviours are blocked. We are currently looking to embed a wide-ranging digital strategy which will be informed in part by this guidance from the UK Safer Internet Centre.

Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An example incident report log can be found in appendix 4.

This policy will be reviewed every year by the DSL. At every review, the policy will be shared with the Senior Leadership Team. The policy review will be supported by self-review tools, such as 360safe, and will include an annual risk assessment that considers and reflects the risks students face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

Links with other policies

This policy statement should be read alongside our organisational policies and procedures, including:

- TLC Safeguarding Policy and Procedures
- TLC Staff Code of Conduct
- TLC Tutor Code of Conduct
- Privacy and Data Protection Policy
- Whistleblowing Policy
- Complaints Policy
- TLC Reporting Safeguarding Concerns Form

Guidance:

- Safeguarding children who come from Black, Asian and minoritised ethnic communities.
- Safeguarding d/Deaf and disabled children and young people.
- Safeguarding LGBTQ+ children and young people.
- Safeguarding children with special educational needs and disabilities (SEND).

Designated Safeguarding Lead
Name: Owais Yasin
Email: owais@learnerscollective.com

Deputy Safeguarding Officer
Name: Rory Gaskin
Email: rory@learnerscollective.com

Deputy Safeguarding Officer
Name: Sian Gaskin
Email: sian@learnerscollective.com

NSPCC Helpline
0808 800 5000

Appendix 1: Acceptable Use Agreement for TLC's Teaching Platform(s) and Microsoft Teams for Students

ACCEPTABLE USE OF THE LEARNERS COLLECTIVE'S TEACHING PLATFORM(S) AND MICROSOFT TEAMS: AGREEMENT FOR STUDENTS AND PARENTS/CARERS

Name of student:

I will use and follow the rules in the acceptable use agreement policy

When I use the organisation's Teaching Platform(s) and Microsoft Teams I will:

- Always use the Teaching Platform(s) and Microsoft Teams responsibly and for educational purposes only
- Keep my username and passwords safe and not share these with others
- Keep my private information safe at all times and not give away any information such as my school name, address or contact details to anyone without the permission of my tutor or parent/carer
- Tell a tutor, my school, my parents/carer/guardian immediately if I find any material which might upset, distress or harm me or others
- Be present in classroom with my microphone and, where necessary, webcam on when requested by the tutor
- Be punctual, joining classes up to 5 minutes before the start time

I will not:

- Access any websites unless my tutor has expressly allowed this as part of a learning activity
- Open any attachments in emails, or follow any links in emails, without first checking with a tutor
- Use any inappropriate language or post any inappropriate content when communicating online, including in emails or messages on the Teaching Platform(s) or during Microsoft Teams tutorials
- Log into the Teaching Platform or Microsoft Teams using someone else's details
- Arrange to meet anyone offline without first consulting with my parent/carer, or without adult supervision

If I have a personal mobile phone or other personal electronic devices with me during class:

- I will not use it during tutorials, unless mu tutor has given me permission for teaching and learning purposes.

I agree that the organisation will monitor my activity on the Teaching Platform(s) and Microsoft Teams tutorials, and that there will be consequences if I do not follow the rules.

Signed (student):	**Date**:

School or parent/guardian/carer agreement: I agree that mu child can use the Teaching Platform(s) and Microsoft Teams when appropriate. I agree to the conditions set out above for pupils using the Teaching Platform(s) and for using personal electronic devices, and will make sure my child understands these.	
Signed (school or parent/guardian/carer):	**Date**:

Appendix 2: Acceptable Use Agreement for TLC's Teaching Platform(s) and Microsoft Teams for TLC Staff and Tutors

ACCEPTABLE USE OF THE LEARNERS COLLECTIVE'S TEACHING PLATFORM(S) AND MICROSOFT TEAMS: AGREEMENT FOR STAFF AND TUTORS	
Name of staff member:	
Role at TLC:	
When I use the organisation's Teaching Platform(s) and Microsoft Teams I will not: • Access, display, upload or share inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) via the Teaching Platform(s) or Microsoft Teams • Use them in any way which could harm the organisation's reputation • Access social networking sites or chat rooms during classes • Use any improper language when communicating online, including in emails, during Teams meetings, or other messaging services • Share my password with others or log in to the Teaching Platform(s) or Microsoft Teams using someone else's details • Take photographs and videos of students and parents • Share confidential information about the organisation, its students or staff, or other members of the community • Access, modify or share data I'm not authorised to access, modify or share • Promote private businesses, unless that business is directly related to TLC I will only use the Teaching Platform(s) or Microsoft Teams for educational purposes or for the purposes of fulfilling the duties of my role. I agree that TLC will monitor my activity on the Teaching Platform(s) or Microsoft Teams. I will take all reasonable steps to ensure that my personal devices are secure and password-protected. I will let the designated safeguarding lead (DSL) and Senior Leadership Team know if a student informs me that they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will report any concerns or issues relating to TLC to my line manager, DSL and Senior Leadership Team where relevant. I will always use the designated Teaching Platform(s) or Microsoft Teams and ensure that students in my care do so too.	
Signed (staff member):	**Date**:

Appendix 3: Online Safety Training Needs – Self Audit for TLC Tutors and Staff

ONLINE SAFTEY TRAINING NEEDS AUDIT	
Name of staff member:	**Date:**
Role at TLC:	
Question	**Yes/No (add comment if necessary)**
Do you know the name of the person who has lead responsibility for online safety at TLC?	
Are you aware of the ways students can abuse other children online?	
Do you know what you must do if a student or parent approaches you with a concern or issue?	
Do you keep your devices and accounts secure?	
Are you familiar with TLC's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

Appendix 4: Example Online Safety Incident Report Log for TLC Tutors

ONLINE SAFTEY INCIDENT LOG				
Date	**Where the incident took place (e.g., website, social media site)**	**Description of the incident**	**Action taken**	**Name and signature of staff member recoding the incident**

Appendix 5: Risk Assessment for Students

Potential Hazard for Students	How Students may be harmed	Protection measures in place	Further measures to take
Harmful or inappropriate material on a tutor's computer.	Students may see harmful or inappropriate material when a tutor uses the screen sharing tool on Microsoft Teams.	Tutors receive extensive, frequent training on what material is harmful or inappropriate for students. Tutors are asked to take care to close all tabs containing harmful or inappropriate content before starting online lessons. Tutors are trained in how to use the screen sharing tool without unintentionally sharing harmful or inappropriate content. Extensive procedures are in place to deal with allegations of misconduct and safeguarding issues involving tutors and online classes. All students have access to tools to report issues that concern them. All Teams video, chats and screen sharing during online	

		classes is recorded and monitored by TLC. Where appropriate, we require students to have an appropriate adult present for the duration of online lessons to act as an additional safeguard.	
Online child-on-child abuse via Zoom classroom tools.	Child-on-child abuse may occur during online classes via the Zoom video, chat, and screen sharing tools. For example, a student may send harmful messages to another student during an online class via the Teams chat tool or share inappropriate images via the screen sharing tool or through changing their Teams background.	Tutors receive extensive, frequent training on how to spot and report child-on-child abuse. All Teams video, chats and screen sharing during online classes is recorded and monitored by TLC. Extensive procedures are in place to deal with allegations of misconduct and safeguarding issues involving tutors and online classes. All students have access to tools to report issues that concern them. Where appropriate, we require students to have an appropriate	

		adult present for the duration of online lessons to act as an additional safeguard. Tutors are trained to “claim host” and present students accessing screensharing tools and private messaging without permission.	
Online child-on-child abuse via other online channels, such as social media and email	Students may experience abuse or harm from other children via online channels outside of TLC control during online classes. For example, a student may receive harmful messages or inappropriate images from children via social media.	Tutors receive extensive, frequent training on how to spot and report child-on-child abuse. All students have access to safeguarding information on Spring and tools to report issues that concern them.	
Online abuse from adults via other online channels, such as social media and email.	Students may experience abuse or harm from adults via online channels outside of TLC control during online classes. For example, a student may receive harmful messages or inappropriate images from adults via social media.	Tutors receive extensive, frequent training on how to spot and report safeguarding concerns, including those arising from online interactions. All students have access to tools to report issues that concern them. We provide information to schools and parents about online	

		safety and ways to keep students safe online. Most schools we work with have internet security measures to prevent students accessing harmful or inappropriate material online.	
Harmful or inappropriate material on the internet, such as web pages and video content that students may access themselves purposefully or inadvertently	Students may be exposed to harmful or inappropriate material on the internet during online classes if they are browsing the internet without the tutor's knowledge, permission or observation.	Tutors receive extensive, frequent training on how to spot and report safeguarding concerns, including those arising from online interactions. All students have access to tools to report issues that concern them. We provide information to schools and parents about online safety and ways to keep students safe online. Most schools we work with have firewalls and internet security measures to prevent students accessing harmful or inappropriate material online.	

Harmful or inappropriate material in a tutor's or other students' video or sound, such as background images or sound.	Students may unintentionally be exposed to harmful or inappropriate images or sounds that appear in others' video streams. For example, the entrance of another person in the video or background noise.	Tutors receive extensive, frequent training on what environments are suitable for online teaching Tutors are instructed never to conduct lessons in public places or areas with other people present. Tutors are encouraged to 'self-report' any instances or interruptions during lessons which could be considered a safeguarding concern. Tutors and students are encouraged to use the 'background blurring' tool or 'background image' tool on Teams if they do not have a neutral background for lessons. Tutors and students are encouraged to use headphones if there is a risk of background noise during lessons	Provide more detailed training for tutors on how to enable the 'background blurring' tool or 'background image' tool on Teams.

		Students, schools and parents are asked to find a quiet, private place for lessons.	
An unauthorised guest in the Teams classroom.	Safeguarding issues may arise if an unauthorised guest enters the Zoom classroom.	Teams link and passwords are only shared via Tutocruncher and are not publicly available online, which reduces the risk that an unauthorised person would gain access. The 'waiting room' is enabled on all Teams classrooms and tutors are trained to only allow students into the classroom who they know should be attending the class. Tutors, as host, can mute individuals and turn off their videos. They can also remove an individual from the online classroom if required. All Teams classes are recorded, and tutors are trained to report any safeguarding concerns, including instances where an unauthorised person enters the Teams classroom.	

Appendix 6s: **Roles and responsibilities in relation to filtering and monitoring**

Role	**Responsibility**
Managing Director	Strategic responsibility for filtering and monitoring and need assurance that the standards are being met.
Technology Lead	Responsible for ensuing these standards are met: and: • Procuring filtering and monitoring systems • Documenting decisions on what is blocked or allowed and why • Reviewing the effectiveness of the filtering and monitoring provision • Overseeing reports • 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. Ensure that all staff: • Understand their role • Are appropriately trained • Follow policies, processes and procedures • Act on reports and concerns
Designated Safeguarding Lead	Lead responsibility for safeguarding and online safety, which could include overseeing and acting on: • Filtering and monitoring reports • Safeguarding concerns • Checks to filtering and monitoring systems • Supporting the Technology Lead in ensuring that staff understand this policy and that it is being implemented consistently throughout the school; • Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy;
IT Manager	Technical responsibility for:

	• Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online, including terrorist and extremist material; • Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
All Staff	Responsible for: • Maintaining an understanding of the online safety policy, including their role in relation to filtering and monitoring • Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with the online safety policy.