Online Safety Policy

Signed	
Position	**Head of School**
Date Agreed	**September 2024**
Next Review	**September 2025**

Equality Statement: Centre Academy London is committed to a policy of equality and aims to ensure that no employee, job applicant, pupil or other member of the school community is treated less favourably on grounds of sex, race, colour, ethnic or national origin, marital status, age, sexual orientation, disability or religious belief. We provide a safe, supportive and welcoming environment.

Centre Academy London (CAL) is committed to safeguarding and promoting the welfare of children and young people and expects all staff to share this commitment.

Contents

1. Online Policy Statement

Centre Academy London recognizes that Online safety is paramount when adults, young people or children are using the internet, social media or mobile devices. The policy statement applies to all staff, volunteers, children and young people and anyone involved in Centre Academy London (CAL) activities.

The purpose of this policy statement is to:

- ensure the safety and wellbeing of children and young people is paramount when adults, young people or children are using the internet, social media or mobile devices
- provide staff and volunteers with the overarching principles that guide our approach to online safety
- ensure that, as an organisation, we operate in line with our values and within the law in terms of how we use online devices.

1.1 Legal framework

This policy has been drawn up on the basis of legislation, policy and guidance that seeks to protect children in England.

Summaries of the key legislation and guidance are available on:

- Online abuse

Protecting children from online abuse | NSPCC Learning

- Bullying

Protecting children from bullying and cyberbullying | NSPCC Learning

- Child abuse and neglect

Protecting children from bullying and cyberbullying | NSPCC Learning

- Child protection

Child protection system for England | NSPCC Learning

We believe that:

- Children and young people should never experience abuse of any kind
- Children should be able to use the internet for education and personal development, but safeguards need to be in place to ensure they are kept safe at all times.

We recognise that:

- The online world provides everyone with many opportunities; however, it can also present risks and challenges
- We have a duty to ensure that all children, young people and adults involved in our organisation are protected from potential harm online
- We have a responsibility to help keep children and young people safe online, whether or not they are using Centre Academy's network and devices
- All children, regardless of age, disability, gender reassignment, race, religion or belief, sex or sexual orientation, have the right to equal protection from all types of harm or abuse
- Working in partnership with children, young people, their parents, carers and other agencies is essential in promoting young people's welfare and in helping young people to be responsible in their approach to online safety.

We will seek to keep children and young people safe by:

- Appointing an online safety coordinator
- Providing clear and specific directions to staff and volunteers on how to behave online through our behaviour code for adults
- Supporting and encouraging the young people using our service to use the internet, social media and mobile phones in a way that keeps them safe and shows respect for others
- Supporting and encouraging parents and carers to do what they can to keep their children safe online
- Developing an online safety agreement for use with young people and their parents/carers
- Developing clear and robust procedures to enable us to respond appropriately to any incidents of inappropriate online behaviour, whether by an adult or a child/young person

1.2 Summary of Changes

The updated definition of safeguarding (in line with the updated 'Working Together to Safeguarding Children' guidance) in part one now explicitly includes recognition that children may be maltreated online.

- The DSL has overall responsibility for safeguarding and child protection, including online safety and understanding the filtering and monitoring systems and processes in place; they can be supported by appropriately trained deputies and should liaise with other staff as appropriate, but this responsibility cannot be delegated.
- DSLs should evidence that they have accessed appropriate training and/or support to ensure they understand the unique risks associated with online safety, can recognise the additional risks learners with SEN and disabilities (SEND) face online, and have the relevant knowledge and up to date capability required to keep children safe online.
- All staff (including governors and trustees) should receive appropriate safeguarding and child protection training, including online safety at induction. This should amongst other things, include an understanding of the expectations, applicable roles, and responsibilities in relation to filtering and monitoring.
- Online safety should also be addressed as part of regular (at least annual) child protection training and staff should receive updates, as appropriate.
- Children should be taught about online safety, including as part of statutory Relationships and Sex Education (RSE), however schools and colleges should recognise that a one size fits all approach may not be appropriate, and a more personalised or contextualised approach for more vulnerable children e.g., victims of abuse and SEND, may be needed.
- Schools/colleges should be doing all that they reasonably can to limit children's exposure to risks from the school's or college's IT system and should ensure they have appropriate filtering and monitoring systems in place and regularly review their effectiveness. The leadership team and relevant staff should have an awareness and understanding of the filtering and monitoring provisions in place and manage them effectively and know how to escalate concerns identified. When making filtering and monitoring decisions, schools/colleges should consider those who are 'potentially at greater risk of harm' and how often they access the IT system along with the proportionality of costs versus safeguarding risks.
- Schools/colleges should recognise that child-on-child abuse, including sexual violence and sexual harassment can occur online. School/colleges have an essential role to play in both preventing online child-on-child abuse and responding to any concerns when they occur,

even if they take place offsite and should have appropriate systems in place to support and evidence this.

- Schools/colleges should ensure their child protection policy and wider safeguarding policies specifically address online safety, especially with regards to appropriate filtering and monitoring on school devices and school networks, child-on-child abuse, relationships on social media and the use of mobile and smart technology.
- Schools/colleges should consider carrying out an annual review of their approach to online safety, supported by an annual risk assessment that considers and reflects the specific risks their children face.

2. Aims

Our school aims to:

Provide an education to our pupils about E-Safety, teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet technologies in and beyond the classroom.

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

The 4 key categories of risk

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

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as child on 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/or financial scams

2. Legislation and guidance

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

- Teaching online safety in schools

- Preventing and tackling bullying and cyber-bullying: advice for Head of Schools and school staff
- Relationships and sex education
- Searching, screening and confiscation

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

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

The policy also takes into account the National Curriculum computing programmes of study.

3. Roles and responsibilities

3.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the heads of school to account for its implementation.

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

The governor who oversees online safety in CAL is: **Lisa Gilbert**
Governors will:

- The governing board will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.
- The governing board will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.
- The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).
- The governing board should ensure children are taught how to keep themselves and others safe, including keeping safe online.
- The governing board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting those standards, which include:
- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

All governors will:

- Ensure they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3)
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school or college approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (Appendix 1 and 2)
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some 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

3.2 The Head of School

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

3.3 The Designated Safeguarding Lead (DSL)

Details of the school's designated safeguarding lead (DSL) Halima Shaker, the Deputies Ms Lee-Douglas & Ms Palamartsuk 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 school, in particular:

- Supporting the Head of School in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Head of School and governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with the ICT Lead to make sure the appropriate systems and processes are in place
- Working with the Head of School, ICT Lead and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school's child protection policy
- Ensuring that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety (appendix 3 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary

- Providing regular reports on online safety in school to the Head of School and/or governing board
- Undertaking annual risk assessments that consider and reflect the risks children face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

3.4 The ICT Lead

The ICT Lead is responsible 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 while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a **weekly** basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged (Appendix 4) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.5 All staff and volunteers

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

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by informing the ICT Lead, Head of School and the Proprietor
- Following the correct procedures by logging on to the London Grid for Learning USO, if they need to bypass the filtering and monitoring systems for educational purposes
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

3.6 Parents

Parents/carers are expected to:

- Notify a member of staff or the Head of School of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2)
- Parents/carers can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International
- Healthy relationships – Disrespect NoBody campaign - GOV.UK (www.gov.uk)
- Parent information about the internet - Parents and carers | CEOP Education (thinkuknow.co.uk)

3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 3).

4. Educating pupils about online safety

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

It is also taken from the guidance on relationships education, relationships and sex education (RSE) and health education. **All** schools have to teach: Relationships education and health education

In **Key Stage 3**, pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns

Pupils in **Key Stage 4** will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

By the **end of secondary school**, pupils will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online

- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

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

As a special needs school, teaching about safeguarding, including online safety, will be adapted for our most vulnerable children, including those who are victims of abuse and developmental delay.

5. Educating parents about online safety

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

Online safety will also be covered during parent consultation evenings.

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

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

The school will let parents/carers know:

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

6. Cyber-bullying

6.1 Definition

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

6.2 Preventing and addressing cyber-bullying

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

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers and mentors will discuss cyber-bullying with their tutor groups.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyberbullying. This includes personal, social, health and economic (PSHE) education, our Rights Respecting School articles based on the UN Convention on the Rights of the Child, Citizenship and other subjects where appropriate.

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

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

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

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

6.3 Examining electronic devices

The Head of School, and any member of staff authorised to do so by the Head of School as set out in our behaviour policy, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence
- Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:
- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the Head of School and/or DSL
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil’s co-operation
- Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a ‘good reason’ to do so.

- When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:
- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or **Commit an offence**

If inappropriate material is found on the device, it is up to the Head of School, DSL and Leadership Team to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

They reasonably suspect that its continued existence is likely to cause harm to any person, and/or

The pupil and/or the parent/carer refuses to delete the material themselves

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

Not view the image

Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with:

The DfE's latest guidance on searching, screening and confiscation

UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Our behaviour policy that outlines searches and confiscation

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

6.4 Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

Centre Academy London recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real.

Centre Academy London will treat any use of AI to bully pupils in line with our behaviour policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the school.

7. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1-3). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

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

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

More information is set out in the acceptable use agreements in appendices 1, 2 and 3.

8. Pupils using mobile devices in school

Pupils may bring mobile devices into school, but are not permitted to use them during:

- Lessons
- Tutor group time
- Clubs before or after school, or any other activities organised by the school
- Mobile phones, smart devices are to be handed in at the gate or into the main office and will returned at the end of the day.
- Any use of mobile devices in school by pupils must be in line with the acceptable use agreement or under teachers' supervision for learning purpose.

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

9. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least **12 characters**, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the **device locks if left inactive** for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date – always install the latest updates

Staff members **must not use** the device in any way which would violate the school's terms of acceptable use, as set out in appendix 3.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from **Mr Angel Okundaye**

10. How the school will respond to issues of misuse

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

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

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

To minimise *issues* of misuse at Centre Academy we've introduced LGfL filtering and monitoring services, which is aligned with The Keeping Children Safe in Education policy 2023, ensuring students are unable to access harmful content, including inappropriate advertisement. For this to be successfully implement to ensure student and staff safety, devices connected 3, 4 or 5G are at risk of exposure to harmful content online. We remind students, parents, visitors, staff, and volunteers to adhere to the acceptable use policy that outlines consequences taken if misuse occurs.

11. Training

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

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

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

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

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

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

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training. This will be carried out **every year.**

Volunteers will receive appropriate training and updates, if applicable.

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

12. Monitoring arrangements

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

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

At Centre Academy we monitor risks pupils face online through their understanding of the digital world through Safe Skills – operated by LGfL. Safe Skills tests students on their competence online and ensures they are confident navigating away from harmful content online. Reports generated informs our annual risk assessment in addition to other records kept such as the incident report log.

Centre Academy London uses Classroom.cloud as our monitoring system; maintaining a safe and secure learning environment at all times has never been more important. With the optional online safety toolkit, selected staff can monitor online activity, identify students at risk, and spot concerning trends. Its powerful tools are perfect for helping to inform our online safety strategy/policies and meeting the latest requirements.

12.1 Key features of Classroom.cloud

- Share your screen and audio to help explain lesson activities
- Monitor students’ screens to ensure they’re on task
- Deliver support quickly and easily via the help request tool
- Give every student a voice with chat and messaging tools
- Use surveys to gamify assessment
- Control website and application usage
- Launch websites and applications directly on students’ devices to help save time
- Remote control students' screens to remedy activity

- Control the use of USBs/webcam/audio during class
- Lock their screens to gain attention
- Power off, Restart or Log out class devices either individually, a selected number, or all at once
- Reset students' passwords without IT support
- Remotely login a student device (Windows only)

13. Links with other policies

This online safety policy is linked to our:

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

Appendix 1: KS3 and KS4 pupil acceptable use agreement

Student Acceptable Use Policy Agreement Slip

Signed	
Position	**Head of IT**
Date Agreed	**September 2025**
Next Review	**September 2026**

Centre Academy London understands the importance of children being able to use the internet for education and personal development. This includes social media platforms, games and apps. We aim to support children and young people in making use of these in our work. However, we also recognise that safeguards need to be in place to ensure children are kept safe at all times.

This agreement is part of our overarching **code of behaviour for children and young people and staff and volunteers**. It also fits with our overarching **online safety policy**. If you would like to know more about this, please speak to **Mr Angel Okundaye.**

- More information about online safety is available from **learning.nspcc.org.uk/safeguardingchild-protection/online-safety-for-organisations-and-groups**

Young person: please read the following agreement and discuss it with your parents/carers and group leader.

Parents/carers: please read and discuss this agreement with your child and then sign it, ask your child to sign it, and return it to the group leader. If you have any questions or concerns please speak to **The Head of School.**

Young person's agreement

- I will be responsible for my behaviour when using the internet, including social media platforms, games and apps. This includes the resources I access and the language I use.
- I will not deliberately browse, download or upload material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to the group leader.
- I will not send anyone material that could be considered threatening, bullying, offensive or illegal.
- I will not give out any personal information online, such as my name, phone number or address.
- I will not reveal my passwords to anyone.
- I will not arrange a face-to-face meeting with someone I meet online unless I have discussed this with my parents and/or group leader and am accompanied by a trusted adult.
- If I am concerned or upset about anything I see on the internet or any messages that I receive, I know I can talk to **Ms Shaker**.

I understand that my internet use at **Centre Academy London** will be monitored and logged and can be made available to the group leader. I understand that these rules are designed to keep me safe and that if I choose not to follow them, **Centre Academy London** may contact my parents/carers.

Signatures:

We have discussed this online safety agreement and ______________________________________ agrees to follow the rules set out above.

Parent/carer signature……………………….……………………………….

Date ………………………………………………

Young person's signature……………………..................................

Date ………………………………………………

Appendix 2: Parent/Carer acceptable user agreement

Centre Academy London - Network/Internet Consent

Dear Parent/Carer

As part of the school's ICT facilities, we offer students supervised access to the Internet via a filtered and monitored network connection. It is the school's policy that, before being allowed to use the Internet, all students must obtain parental permission and therefore, both they and you are requested to sign and return the enclosed form as evidence of your approval and their acceptance of the school policy and rules on this matter.

Access to the Internet will enable students to explore a vast resource of information but parents should be warned that some material accessible via the Internet may contain items that are illegal, defamatory, inaccurate or potentially offensive.

While our aim for Internet use is to further our students learning, students may find ways to access other material. We believe that the benefits to students from access to the Internet, in the form of information and resources, exceed any disadvantages. The school's on-line safety policy encourages teachers, parents, and pupils to discuss and communicate a shared responsibility of keeping pupils safe. Ultimately though, parents and carers of minors are responsible for setting and conveying the standards that their children should follow when using media and information sources. To that end, the school supports and respects each family's right to decide whether their child should have access.

During lessons, teachers will guide students towards appropriate material. Outside of school, families bear the same responsibility for such guidance as they exercise with information sources such as television, telephones, videos, movies, radio, and other potentially offensive media.

The school policy regarding the use of the network and the Internet has been revised in the light of changing use. We have specifically excluded the use of both chat rooms and games, both of which waste a great deal of time and use up significant network resources. Students must also agree to the conditions shown overleaf every time they log onto the Internet.

We endeavour to keep pupils safe when on-line using ICT. If you have any concerns in this area, please contact our Online Safety Officer or the school office.

If you and your child could both read the ***Acceptable Use Agreement*** on the reverse, complete the permission slip, which follows and then return the whole document to the school.

Acceptable Use of Technology Statements and Form for Parents/Carees

1. I have read and discussed the pupil acceptable use of technology policy (AUP) with my child and understand that the AUP will help keep my child safe online.

2. I understand that the AUP applies to my child's use of school devices and systems on site and at home and personal use where there are safeguarding and/or behaviour concerns. This may include if online behaviour poses a threat or causes harm to another pupil could have repercussions for the orderly running of the school, if a pupil is identifiable as a member of the school, or if the behaviour could adversely affect the reputation of the school.

3. I am aware that any use of school devices and systems are appropriately filtered and may be monitored for safety and security reason to keep my child safe and to ensure policy compliance. This monitoring will be proportionate and will take place in accordance with data protection, privacy, and human rights legislation.

4. I am aware that the school mobile and smart technology policy states that my child cannot use personal device and mobile and smart technology on site. If my child needs to bring in a mobile phone, it should be handed to the office at the start of the day.

5. I understand that the school will take every reasonable precaution, including implementing appropriate monitoring and filtering systems, to ensure my child is safe when they use school devices and systems. I understand that the school cannot ultimately be held responsible for the nature and content of materials accessed online or if my child is using personal mobile or smart technologies.

6. I and my child are aware of the importance of safe online behaviour and will not deliberately upload or share any content that could upset, threaten the safety of or offend any member of the school community, or content that could adversely affect the reputation of the school.

7. I understand that the school will contact me if they have concerns about any possible breaches of the AUP or have any concerns about my child's safety online.

8. I will inform the school or other relevant organisations if I have concerns over my child's or other members of the school community's safety online.

9. I know that my child will receive online safety education to help them understand the importance of safe use of technology and the internet, both in and out of school.

10. I understand my role and responsibility in supporting the school's online safety approaches and safeguarding my child online. I will use parental controls, supervise access and will encourage my child to adopt safe use of the internet and other technology at home, as appropriate to their age and understanding.

Parental Consent for AUP

Name of Student: **Class:**

As the parent or legal carer of the above named student, I grant permission for my child to use electronic mail and the Internet. I understand that students will be held accountable for their own actions. I also understand that some materials on the Internet may be objectionable and I accept responsibility for setting standards for my daughter or son to follow when selecting, sharing and exploring information and media.

Name of Parent/Carer: ………………………………………………… (please print in block capitals)

Parent/Carer Signature: ………………………………………………… **Date**: ……./……../……….

Appendix 3: acceptable use agreement (staff, governors, volunteers and visitors)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS,VOLUNTEERS AND VISITORS

Name of staff member/governor/volunteer/visitor:

When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Use them in any way which could harm the school's reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the school's network
- Share my password with others or log in to the school's network using someone else's details
- Take photographs of pupils without checking with teachers first
- Share confidential information about the school, its pupils 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 the school

I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.

I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.

I will let the designated safeguarding lead (DSL) and ICT Lead know if a pupil informs me 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 always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 3: online safety training needs – self audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	**Date**:
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways pupils can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

Appendix 4: online safety incident report log

ONLINE SAFETY INCIDENT LOG				
Date	**Where the incident took place**	**Description of the incident**	**Action taken**	**Name and signature of staff member recording the incident**