Online Safety Policy

Signed	*[signature]*
Position	**Head of School**
Date Agreed	**September 2023 Updated May 2024**
Next Review	**September 2024**

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

The purpose of this policy statement for Centre Academy London is that works with children and families as part of its activities.

The purpose of this policy statement is to:
-

- Have robust processes in place to ensure the online safety of pupils; staff, volunteers and governors
- Identify and support groups of pupils that are potentially at greater risk of harm online than others
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology including mobile 'pones and watches
- 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.
- To provide staff and volunteers with the overarching principles that guide our approach to online safety and clear mechanisms to identify, intervene and escalate an incident, where appropriate
- Ensure that, as an organisation, we operate in line with our values and within the law in terms of how we use online devices.

2. Legal framework

This policy is based on the Department for Education's (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-bullying: advice for headteachers and school staff

> Relationships and sex education

> Searching, screening and confiscation

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

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

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

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

3. 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

4. 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, 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

5. 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.

6. Roles and responsibilities

6.1 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:

- Have responsibility for monitoring this policy and holding the headteacher to account for its implementation
- 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 duties
- 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 the standards, which include:
  1. Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
  2. Reviewing filtering and monitoring provisions at least annually;
  3. Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
  4. Having effective monitoring strategies in place that meet their safeguarding needs.

The governor who oversees online safety is Ms Lisa Gilbert:

- 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 3)
- 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.

6.2 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.

6.3 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 5) 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 4 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.

6.4 The Online Safety Lead/ICT Manager

The Online Safety Lead/IT Manager is responsible for:

- Ensuring an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist materia, to work closely with Agile Computers to support this, as well as the functional aspects of the systems
- 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
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning
- Ensuring that any online safety incidents are logged in conjunction with the DSL (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 school behaviour policy.
- Ensure children are taught how to keep themselves and others safe, including keeping safe online. This can be taught discretely during Computer Science/IT lessons and PSHERSE lessons.

This list is not intended to be exhaustive.

6.5 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 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 school behaviour policy.
- 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 filling in Appendix 5 (Online Safety Incidence Report log) and informing the DSL and Online Safety Lead
- Follow the correct procedures if they need to bypass the filtering and monitoring systems for educational purposes.
- 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.

6.6 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)](#)

6.7 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).

7. 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 primary schools

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 for example during IT lessons, PSHE, RSE and other lessons that are appropriate.

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.

8. 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.

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

If parents 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.

9. Cyber-bullying

9.1 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*.)

9.2 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 cyberbullying, 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.

9.3 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

9.4 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.

9.5 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.

10. 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.

11. 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 be returned at the end of the day. Students are to switch off their 'phones before entry to the school gate and may only switch them on, when they are outside of the school gates

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.

12. 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 **Mrs S Yar, IT Lead.**

13. 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 have 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 implemented 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.

14. 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 do not 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:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse.
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh the risks up.
- 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.

15. 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.

16.   Links with other policies

This online safety policy is linked to our:
- Child protection and safeguarding policy
- Student Behaviour Policy and Statement of Behaviour Principles 2023-24
- Student Conduct Discipline and Exclusion Policy 2023-24
- Mental Heatlh and Wellbeing Policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Safer Recruitment Policy
- PSHE RSE Policy
- Complaints procedure
- ICT and internet acceptable use policy

Appendix 1: KS3 and KS4 acceptable use agreement (pupils and parents/carers)

<table>
<tr><td colspan="2">ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS</td></tr>
<tr><td colspan="2">Name of pupil:</td></tr>
<tr><td colspan="2">

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

When I use the school's ICT systems (like computers) and get onto the internet in school I will:

- Always use the school's ICT systems and the internet responsibly and for educational purposes only
- Only use them when a teacher is present, or with a teacher's permission.
- Keep my username and passwords safe and not share these with others.
- Keep my private information safe at all times and not give my name, address, or telephone number to anyone without the permission of my teacher or parent/carer.
- Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others.
- Always log off or shut down a computer when I am finished working on it **I will not:**
- Access any inappropriate websites including social networking sites, chat rooms and gaming sites unless my teacher 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 teacher.
- Use any inappropriate language when communicating online, including in emails.
- Log in to the school's network using someone else's details.
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision **If I bring a personal mobile phone or other personal electronic device into school:**
- I will not use it during lessons, tutor group time, clubs or other activities organised by the school, without a teacher's permission.
- I will use it responsibly and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online.

I agree that the school will monitor the websites I visit and that there will be consequences if I do not follow the rules.
</td></tr>
<tr><td>Signed (pupil):</td><td>Date:</td></tr>
<tr><td colspan="2">Parent/carer's agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.</td></tr>
<tr><td>Signed (parent/carer):</td><td>Date:</td></tr>
</table>

Appendix 2: 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 am 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.

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

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?	

: 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**