Centre Academy East Anglia

Online Safety Policy

Equality Statement

Centre Academy East Anglia 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

Review Date: Annually	August 2025
Last Review Date:	July 2024
Held on website:	Yes

Signed by Chair of Proprietor Body

Signed: **Date: 05/07/24**

Chair of Proprietor Body **Mr R Murphy**

Centre Academy East Anglia is committed to safeguarding and promoting the welfare of children and young people and expects all staff to share this commitment.

Online Safety Policy Statement

Centre Academy East Anglia 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 East Anglia (CAEA) activities.

The purpose of this policy statement is to:

- ensure the safety and wellbeing of children and young people
- 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.

Legal framework

- This policy has been drawn up based on legislation, policy and guidance that seeks to protect children in England, Summaries of the key legislation and guidance are available on:
- online abuse learning.nspcc.org.uk/child-abuse-and-neglect/online-abuse
- bullying learning.nspcc.org.uk/child-abuse-and-neglect/bullying
- child protection learning.nspcc.org.uk/child-protection-system

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:
- 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

Contents

1. 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 governance
- 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 peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – 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 scam

2. Legislation and guidance

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

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

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

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

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

3. Roles and responsibilities

3.1 CAEA governance

CAEA Governance has overall responsibility for monitoring this policy and account for its implementation.

Member of Governance responsible for CAEA Safeguarding is Cas Lee-Douglas Head of School Centre Academy London (CAL).

Head of school East Anglia; Lisa Gilbert / ADSL, 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).

All members of Governance will:

- Have responsibility for monitoring this policy
- 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
- Ensure that 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 interrelated theme while devising and implementing a whole school approach to safeguarding and related policies and procedures.
- 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.
- 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).
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and pupils with special educational needs (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.
- 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.

3.2 The Head of School

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

3.3 The Designated Safeguarding Lead

Details of the school's DSL and deputies 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 headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher, online safety lead and other staff, as necessary, to address any online safety issues or incidents
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with the online safety lead to make sure the appropriate systems and processes are in place
- Managing all online safety issues and incidents in line with the school 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
- 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.
- Providing regular reports on online safety in school to the headteacher and CAEA Governance.
- Undertake annual risk assessments with the Online Safety Lead and consider and reflect on 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 Online Safety Lead/ICT manager

The online safety lead/ICT manager is responsible for:

- Ensuring an appropriate level of security protection procedures, such as filtering and monitoring systems and processes are in place on school devices and school networks 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, 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 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)
- 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'
- Understand 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.
- Staff recognise that AI has many uses, including enhancing teaching and learning, and in helping to protect and safeguard pupils. However, AI may also have the potential to facilitate abuse (e.g. bullying and grooming) and/or expose pupils to harmful content. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real.
- CAEA will treat any use of AI to access harmful content or bully pupils in line with this policy and our anti-bullying policy.
- Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out risk assessments for any new AI tool being used by the school.

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2)

Parents 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

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

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

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

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

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 such as RSE, where appropriate.

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

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.

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

Online safety will also be covered during specific parents' evenings.

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

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

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the Behaviour and the Anti -Bullying 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/form teachers will discuss cyber-bullying with their tutor groups.

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

All staff and CAEA Governance 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 headteacher, and any member of staff authorised to do so by the headteacher, 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, the authorised staff member will:

- 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 headteacher/designated safeguarding lead /senior management team.
- 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 cooperation

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 staff member in conjunction with the DSL / headteacher / other member of the senior 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 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

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

* Staff may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse includes an online element.

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.
- CAEA 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. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.
- CAEA will treat any use of AI to bully pupils in line with our anti-bullying policy https://www.centreacademy.net/wp-content/uploads/2024/01/Anti-Bullying-Policy-D23.pdf

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 however, students are required to hand in their Mobile phones at the start of the day at the school gate, these are then collected at the end of the day. If a student does not hand in their mobile phone, and the school suspect they have their phone, then the Head of School/member of SMT will be informed and a bag search will be carried out if required.

Mobil phones are not permitted to be used during the school day such as in:

- Lessons
- Tutor group time
- Clubs before or after school, or any other activities organised by the school

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

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 8 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 the ICT manager.

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.

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:
    - Abusive, harassing, and misogynistic messages
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
    - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- 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, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

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

Volunteers will receive appropriate training and updates, if applicable.

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

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 5. Monitoring will take place through the safeguarding reports provided for the Head of School.

This policy will be reviewed every year by the DSL/ICT Manager. At every review, the policy will be shared with CAEA Governance. The review will 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.

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: Student acceptable use agreement (pupils and parents/carers)

Centre Academy East Anglia – Student Acceptable Use Agreement

Name of Student: Class:

The school computer system is made available to students to enhance and supplement their learning. This Acceptable Use Agreement has been produced to protect everyone concerned - the students, the staff and the school.

The school reserves the right to examine and if necessary delete any files that may be held on its computer system and to monitor Internet sites visited.

Students should sign below to confirm that they have read and agree to the following conditions:

1. I will only use ICT systems in school, including the internet, e-mail, digital video, and mobile technologies for school purposes.

2. I will not take part in any activity that threatens the integrity of the school computer network, or that attempts to attack or corrupt any other system. I will not attempt to bypass the internet filtering system.

3. I will only open / delete my own files in my folder and student data area.

4. I will not give my name, personal details, phone number, address or details of the school or any information that might identify me to any third parties on the Internet.

5. I will not use chat rooms (including MSN) or send text messages to mobile phones.

6. I will not play computer games unless part of an ICT lesson or in activities time (boarding).

7. I will not download or install software or music files on school technologies. I will not upload or forward material that could be considered offensive or illegal.

8. I will give explicit credit for any material included in my work that has been obtained from CD-ROMS and websites respecting the ownership of other's work.

9. I will use the same high level of courteous and polite language when using e-mail and communications as is expected of me throughout the school.

10. I will not use the network to access or attempt to access inappropriate material that may be considered pornographic, racist or offensive.

11. I will report unsuitable material to a member of staff immediately.

12. I will only log on to the Internet or the network with my own username or password.

13. I will not reveal my passwords to anyone.

14. I will only use my school email address for school work.

15. I am aware that when I take images of pupils and/ or staff that I must only store and use these for school purposes. I must never distribute these outside the school network without permission of all parties involved. This includes school breaks and all occasions when I am in a school uniform or when otherwise representing the school.

16. I will support the school approach to online safety and not upload or add any images, videos, sounds or text to social media that could upset and member of the school community.

17. I will not sign up to on-line services until I am old enough to do so.

18. I understand many of these rules are designed to keep me safe.

Breaking these conditions may lead to a temporary or permanent ban on the use of the school computer network. Students violating the **Computer Misuse Act (1990)** or the **Copyright, Designs and Patents Act (1988)** will be reported to the appropriate authorities.

I agree to accept the conditions outlined above:

Student's Signature: …… Date: ……/……../…….

Appendix 2: Parent/Carer acceptable user agreement

Centre Academy East Anglia
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 network connection. It is the schools 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 or not 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 (including MSN) 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 On-line 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.

Parental Consent

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

Centre Academy East Anglia

Staff Acceptable Use Agreement

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with Mr Curtis– On-Line Safety Officer.

- I will only use the school's email and internet and any related technologies for professional purposes or for uses deemed acceptable by the Head or Governing Body
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role
- I will not give out my own personal details, such as mobile phone number, personal e-mail address, personal Twitter account, or any other social media link, to pupils
- I will ensure that personal data (such as data held on the staff document server) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body. Personal or sensitive data taken off site must be encrypted, eg on a password secured laptop or memory stick
- I will not install any hardware or software without permission.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member
- Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher
- I will support the school approach to online safety and not upload or add any images, video, sounds or text linked to or associated with the school or its community'
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request to my Headteacher
- I will respect copyright and intellectual property rights
- I will ensure that my online activity, both in school and outside school, will not bring the school, my professional reputation, or that of others, into disrepute
- I will support and promote the school's e-Safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies
- I will not use personal electronic devices (including smart watches) in public areas of the school during my contracted work times.
- I understand this forms part of the terms and conditions set out in my contract of employment

User Signature

I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school

Signature …… Date ……

Full Name …….... (printed)

Job title ……

Appendix 4: 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 5: 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**