# Centre Academy East Anglia

# E - Safety (Online Safeguarding) 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

To be reviewed annually

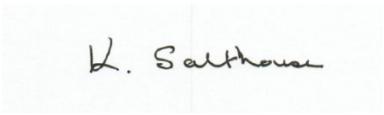
Next review date: Sept 2021

Displayed on Website

**Signed:** 

**Date: 01/09/20**

**Principal and CEO** **Dr Rollo**

**Signed:** 

**Date: 01/09/20**

**Head of School** **Mrs Salthouse**

*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.*

**Introduction**
ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment. In this light parents are initially approached for permission for pupils to:

1. use their child's photograph in the school prospectus and other printed publications that we produce for promotional purposes or on project display boards.
2. use their child's image on our website
3. record their child's image on video
4. they are happy for their child to appear in the media

Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

Websites
Apps
E-mail, Instant Messaging and chat rooms
All Social Media, including Facebook and Twitter
Mobile/Smart phones with text, video and/or web functionality
Other mobile devices including tablets and gaming devices
Online Games
Learning Platforms and Virtual Learning Environments
Blogs and Wikis
Podcasting
Video sharing
Filming
Photography
Downloading
On demand TV and video, movies and radio/smart TVs

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies and that some have minimum age requirements (13 years in most cases).

At **Centre Academy East Anglia,** we understand the responsibility to educate our pupils about E - Safety Issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Schools hold personal data on learners, staff and others to help them conduct their day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in media coverage, and potentially damage the reputation of the school. This can make it more difficult for the school to use technology to benefit learners. The school is aware of its legal responsibility to follow the requirements of the Data Protection Act 1998 and of the GDPR.

Everybody in the school community has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

Both this policy and the Acceptable Use Agreement (for staff, governors, and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, mobile devices, webcams, whiteboards, camera's, voting systems, digital video equipment, etc); **and technologies**

**owned by pupils** and staff, but brought onto school premises (such as laptops, mobile phones and other mobile devices).

**Pupils who bring their own devices to school must still follow the Acceptable Use Agreement when using their devices.**

**Development Monitoring and Review**
Due to the ever changing nature of digital technologies, it is best practice that the school reviews the E - Safety Policy at least annually and, if necessary, more frequently in response to any significant new developments in the use of the technologies, new threats to E - Safety or incidents that have taken place.

As part of this monitoring and review the school policy on mobile phones has now been altered for the boarding students. Discussions have taken place within the boarding houses and with Care Staff, Dr Rollo, Mrs Salthouse, and Mr Thompson.

The final compromise agreement has been that students are now able to use their mobile phones for the majority of the evening time. These will then be returned to the Head of House before everyone retires.

Day students who bring their mobile phones to school hand them in to the office at the start of the day and pick them up shortly before they leave school.

Access to the internet during the evenings has also been re-addressed and is available for those who request it.

The implementation of this E - Safety policy will be monitored by the: *E - Safety Officer / Designated Safeguarding Lead / Senior Leadership Team, the Principal and the Head of School*
Monitoring will take place at regular intervals: Annually (see above)

The Governance Board will receive a report on the implementation of the E – Safety Policy generated by the monitoring group (which will include anonymous details of E - Safety incidents) at regular intervals: Annually.

Should serious E - Safety incidents take place, the following external persons / agencies should be informed: Police, see Anti Bullying Policy, Suffolk Safeguarding Children's Board, Social Services. (Refer to Safeguarding Policy

The school will monitor the impact of the policy using:

- *Logs of reported incidents*
- *monitoring logs of internet activity (including sites visited)*
- *Internal monitoring data for network activity*
- *Surveys / questionnaires of*
  - *students / pupils*
  - *parents / carers*
  - *staff*

This policy applies to all members of the school community (including staff, students/ pupils, and parents / carers who have access to and are users of school ICT systems, both in and out of CAEA.

The Education and Inspections Act 2006 empowers Head teachers / Principals to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e - safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix for CAEA policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

It is considered that Staff also need to be aware that under 'the Malicious Communications Act 1988, it is an offence for a person to send an electronic communication to another person with the intent to cause distress or anxiety…'

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e - safety behaviour that take place out of school.

**Monitoring**
All internet activity is logged by the schools internet provider, and reports generated from the Cyberoam firewall are supported by Ipswich Computers.

ICT authorised staff may monitor, intercept, access, inspect, and disclose telephone calls, e-mails, instant messaging, internet/intranet use and any other electronic communications (data, voice, video or image) involving its employees or pupils, without consent, to the extent permitted by law. This may be to confirm or investigate compliance within school policies, standards and procedures; to ensure the effective operation of school ICT; to comply with a Subject Access Request under the Data Protection Act 1998, or to prevent or detect crime.

A breach or suspected breach of policy by a pupil or school employee may result in the temporary or permanent withdrawal of school ICT hardware, software or services from the individual. (Reference the schools Behaviour Policy)

All security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the Head of ICT and the main office. Additionally, all security breaches, lost/stolen equipment or data (including passwords etc.), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the relevant responsible person.

Also please see diagram 'Responding to Incident of Misuse'. (Attached)
The relevant responsible individuals at CAEA are:

Mr W Pipe – E-Safety Officer and Head of ICT
Mrs L West – Secretary to the Head of School (who will liaise with Ipswich Computers)
Mrs K Salthouse – Head of School
Dr D Rollo – CEO/Principal

**Roles and Responsibilities**
An effective School E - Safety Policy must be tailored to the needs of each school and an important part of the process will be the discussion and consultation which takes place during the writing or review of the policy. This will help ensure that the policy is owned and accepted by the whole school community.

Consultation in the production of this policy involved:
Governance
Teaching Staff and Support
Students / pupils
Parents (to be sent home when completed)

**Governance:**
Governance are responsible for the approval of the E - Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governance receiving regular information about e - safety incidents and monitoring reports. A member of the Governance Board has taken on the role of *E - Safety* Governor (it is suggested that the role may be combined with that of the Child Protection / Safeguarding Governor). The role of the E - Safety Governor will include:

- regular meetings with the e - safety officer
- regular monitoring of on-line safety incident logs
- regular monitoring of filtering

- reporting to relevant Governance

**Head of School / Principal/ SLT:**

- The Head of School and/ or Principal has a duty of care for ensuring the safety (including on-line safety) of members of the school community, though the day to day responsibility for on-line safety will be delegated to the *E - Safety Officer.*
- The Head of School and (at least) another member of the Senior Leadership Team / Senior Management Team, DSL, should be aware of the procedures to be followed in the event of a serious on-line safety allegation being made against a member of staff. (see Managing Allegations Policy) The Head of School / Principal / Senior Leadership Team will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal on-line safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles. At CAEA the SMT/ Head of School and the Principal will all provide support and advice to the E - Safety Coordinator. Additionally the DSL will contact the SSCB for advice in the event of findings relating to a member of CAEA or of an allegation against a member of staff relating to on-line safety. (As above)
- The Senior Leadership Team / Senior Management Team will receive regular (termly) monitoring reports from the E - Safety Officer.

The e - safety committee will consist of:
Mr W Pipe – E-Safety Officer and Head of ICT
Mrs A Shaul – DSL
Mr A Thompson – Head of Care (Welfare)

- Mr Pipe takes day to day responsibility for on-line safety issues and has a leading role in establishing and reviewing the school on-line safety policies / documents
- Mrs Shaul ensures that all staff are aware of the procedures that need to be followed in the event of an on-line safety incident taking place.
- Both provide training and advice for staff
- Mrs Shaul liaises with the Local Authority / relevant body
- Mr Thompson liaises with school technical staff
- Mr Pipe receives reports of on-line safety incidents and creates a log of incidents to inform future on-line safety developments,
- Mr Pipe meets regularly with On-line safety Governor to discuss current issues, review incident logs and filtering / change control logs
- All report regularly to Senior Leadership Team/ Head of School/ Principal

**The Co-ordinator for ICT** and the service provider for the schools ICT is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required on-line safety technical requirements and any Local Authority Guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- the filtering policy, is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that they keep up to date with e - safety technical information in order to effectively carry out their on-line safety role and to inform and update others as relevant
- that the use of the network / internet / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Head of School / Principal/DSL/Head of Care for investigation / action / sanction
- that monitoring software / systems are implemented and updated

**Teaching and Support Staff** are responsible for ensuring that:

- they have an up to date awareness of e - safety matters and of the current school e - safety policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy

- they report any suspected misuse or problem to the Head of School / Principal / On-line safety Coordinator for investigation / action / sanction
- all digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official school systems
- e - safety issues are embedded in all aspects of the curriculum and other activities
- students / pupils understand and follow the on-line safety and acceptable use policies
- students / pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

**Safeguarding Designated Lead/ Alternate**
Should be aware of e - safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

Students / pupils:
- are responsible for using the school technology systems in accordance with the Student / Pupil Acceptable Use Policy
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying
- should understand the importance of adopting good on-line safety practice when using digital technologies out of school and realise that the school's E - Safety Policy covers their actions out of school, if related to their membership of the school.

**E - Safety Skills for Staff**
Our staff to receive regular information and training on E - Safety and how they can promote the 'Stay Safe' online messages. This is addressed through guidance from the E - Safety Officer, with presentations and INSET.

**Parents / Carers**
Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' days, coffee mornings, newsletters, letters, website and information about national / local on-line safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good on-line safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- their children's personal devices in the school

**Policy Statements**
Education – students / pupils

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment. However, to support and protect our students the following conditions are to be followed.

- Accessing, creating, transmitting (sending), displaying or publishing any material (e.g. images, sounds or data) that is likely to cause offence, break copyright (or other data protection regulations), inconvenience or needlessly cause anxiety is not permitted.
- Reporting to the Principal, Head of School or other senior teacher any vulnerability in the system or any inappropriate or offensive communications.
- Transmitting unsolicited material to other users (including those on other networks)e.g. sending of mass emails (spam) is not permitted. Peer to peer file sharing is also not permitted as it often involves illegal material and uses excessive bandwidth.
- Older students are expected to act in a responsible and caring way to younger students and must not attempt to mislead or corrupt through exposure to inappropriate content.
- Accessing or attempting to access any data or resources on the school network system or other systems which knowingly have not been explicitly permitted is not permitted.
- Network storage is principally for work. Whilst it is understood that users can store personal content on the network they must understand that this can be accessed by others.
- Not tampering with any aspects of the school system hardware or software setup. This includes, but is not exclusive to, the installation of software. Use of portable hard disks and memory sticks is allowed but not the running of unauthorised executable files from these devices.
- Students are not permitted to create bespoke wireless networks between student devices that have not been sanctioned by the Principal or Head of School.
- All students will accept responsibility for any communication from their personal account and any material this communication may contain.
- Respecting the fact that computer rooms are first and foremost places of work. Eating, drinking, loutish behaviour, listening to music (even with headphones unless permitted by a teacher) or any behaviour which may disturb others from their work is strictly forbidden in the computer room and users will be asked to leave if found so doing.

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be reported immediately to the E - Safety Officer or the Head of School/ Principal. Computer misuse can constitute a serious offense under the Computer Misuse Act, 1990.

**Curriculum**

E - Safety should be a focus in all areas of the curriculum and staff should re-enforce on-line safety messages across the curriculum. The on-line safety programme should be broad, relevant and provide progression with opportunities for creative activities and will be provided in the following ways.
All students will follow the curriculum from Childnet E-safety at Key Stages 1, 2, 3 and 4 while using current resources from Childnet and CEOPs. E - safety issues are taught alongside annual teaching, Safer Internet Day, relating to the internet and e-mail.

A planned e - safety curriculum should be provided as part of ICT , PHSE and other lessons and should be regularly revisited;

- Key on-line safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- An ICT Code of Conduct is included in this policy. A hard copy is kept available at all times in the ICT room and is displayed predominantly.
- Students / pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Students / pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students / pupils should be helped to understand the need for the student / pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school

- Staff should act as good role models in their use of digital technologies the internet and mobile devices
- In lessons where internet use is pre-planned, it is best practice that students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where students / pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Whilst Centre Academy recognises the need to respect privacy, users should not expect that emails, files stored on servers or disks will always be private. Student files held on the school's network may be accessed by any member of the teaching staff at any point.

Personal phones and text messaging also fall under School rules (see below) Mobile phones are not permitted in the school week. (See mobile phone appendix)

**SPECIFIC RULES REGARDING INTERNET USE**

Access to the Internet must only be made via a user's authorised account and password, which must not be given to or shared with any other person.

Students should observe the rules of netiquette at all times just as they are expected to behave well in a classroom or a corridor.

- Not using someone else's name and pretending to be them.
- Not posting or distributing material that is deemed illegal.
- Not using abusive or threatening language (this includes the use of internet slang)
- Not posting racist remarks regarding people's sex, race or gender.
- Not spamming message boards or chat rooms with useless or repeated messages.
- Not trying to obtain or use someone else's password.
- Not trying to obtain personal information about someone

During the working day students may only access or download and save material from sites to support specifically school related work, projects or school activities authorised by staff. In leisure time (which includes lunch and morning break) students are permitted to access appropriate content in keeping with House rules and regulations.

As use of the Internet will be specifically identified with Centre Academy East Anglia the school reserves the right to review files and communications and to monitor and report student use to ensure that users are using the system responsibly.

Students are not permitted to attempt to circumvent the school's filtering system by the use of proxy servers or any other methods. Students are expected to respect the spirit of the rules regarding Internet use and not to attempt to access the type of sites which they know are not permitted either at all or at certain times of the school day.

Students are not permitted to waste Internet time and leave themselves logged on. Indeed, leaving pcs switched on and logged on whilst not being used is an excessive waste of energy.

**SOME SPECIFIC ADVICE FOR INTERNET USE**

Never tell anyone you meet on the Internet your home address, your telephone number or your school's name, unless a member of staff gives you specific permission. Identity theft is also a real problem.

Social networking is a tool for keeping in touch, enjoyment and informal learning. It should never be a method to air grievances or defame another individual. Social networking sights should not be accessed at school.

Remember that all communication on the Internet, statements made or personal details released leave an electronic trail and are in the public domain over which you may have no control. Users are advised to exercise real discretion in befriending online.

Never send your picture to anyone over the Internet without the permission of a member of staff.

Never give your password to anyone, even your best friend.
Never answer nasty, suggestive or rude e-mails; report them to staff.
Always tell the member of staff if you see bad language or unpleasant pictures whilst on line.
Always be yourself and never pretend to be anyone or anything that you are not.

**SANCTIONS**
Breaking any of the above rules may result in a temporary, or permanent, ban on network or Internet use. Or result in the confiscation of personal devices such as laptops and i-pads.

Additional disciplinary action may be added in line with other existing school rules and practices, for example, related to bullying. Action may therefore also include warnings, suspension of user access - temporary and permanent, school detentions or other appropriate punishments and finally temporary and or permanent exclusions from school.

**Appendix 1**
**Mobile Phone Code**
It is now unrealistic to suppose that mobile devices are brought to School by only those pupils who genuinely need to communicate with parents or others about travel and other logistical arrangements, or for whom they enhance security and safety while travelling home. Given that the ownership of mobile phones is wide-spread, the following conditions apply for their use at School:

**Procedure:**
The School recognizes mobile devices as a convenient means of communication, with obvious health and safety benefits. Unfortunately, they can have an intrusive and disruptive effect on community life, therefore, they are banned during the school day, except for particular circumstances. The School encourages communication, especially with parents and carers, and in this light has installed additional telephone lines to ensure that students are always able to make calls.

Pupils who carry mobile devices are to hand these into the Head of Care or Housemaster for safekeeping during the school day.
Boarding students are allowed to request their mobile phones during the evening provided they are returned to the Head of House before the student retires to bed.

On some school trips pupils will be allowed to carry mobile devices, but this will be decided by the member of staff organizing the trip.

*As with normal telephone calls, staff should never make or receive calls on a mobile device during class unless in an absolute emergency.

*Mobile devices should never be used to take photographs of other pupils.

The School reserves the right to immediately confiscate a mobile device from any pupil who contravenes any of the above. The mobile device should be handed into the school office in an envelope with the pupil's name on it and should only be returned by the pupil's Housemaster/Head of Care/form teacher. Any contravention of the policy on photography will be treated extremely seriously.

The School is not responsible for the investigation of any incident of a mobile device being stolen, lost or damaged, either wilfully or accidentally. Pupils entrusted with a mobile device should acknowledge their

responsibility for its security. Neither will the School be responsible for or investigate any misuse of a mobile device by another pupil.

**Appendix 2**

The use of e-mail within most schools is an essential means of communication for both staff and pupils. In the context of school, e-mail should not be considered private. Educationally, e-mail can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school or international. We recognise that pupils need to understand how to style an e-mail in relation to their age and how to behave responsible online.

**Managing e-mail**

- The school gives all staff & governors their own e-mail account to use for all school business as a work based tool This is to protect staff, minimise the risk of receiving unsolicited or malicious e-mails and avoids the risk of personal profile information being revealed
- Staff should use their school email for all professional communication.
- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary e-mail histories can be traced. The school email account should be the account that is used for all school business
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal e-mail addresses
- All e-mails should be written and checked carefully before sending, in the same way as a letter written on school headed paper
- Staff sending e-mails to external organisations, parents or pupils are advised to cc. the Head of School, or designated line manager
- Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes
- E-mails created or received as part of your school job will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000. You must therefore actively manage your e-mail account.
- The following pupils have their own individual school issued accounts ***(list groups of children or individuals attached)***.
- The forwarding of chain emails is not permitted in school.
- All pupil e-mail users are expected to adhere to the generally accepted rules of responsible online behaviour particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission, virus checking attachments
- Pupils must immediately tell a teacher/ trusted adult if they receive an offensive or upsetting e-mail
- Staff must inform (the On-line Safety Officer/ Secretary ) if they receive an offensive e-mail
- Pupils are introduced to e-mail as part of the Computing Programme of Study
- However you access your school e-mail (whether directly, through webmail when away from the office or on non-school hardware) all the school e-mail policies apply

**Sending e-mails**

- Use your own school e-mail account so that you are clearly identified as the originator of a message
- Keep the number and relevance of e-mail recipients, particularly those being copied, to the minimum necessary and appropriate
- Do not send or forward attachments unnecessarily.
- School e-mail is not to be used for personal advertising

**Receiving e-mails**

- Check your e-mail regularly
- Never open attachments from an untrusted source.
- Do not use the e-mail systems to store attachments. Detach and save business related work to the appropriate shared drive/folder

**e-mailing Personal, Sensitive, Confidential or Classified Information**

- Where your conclusion is that e-mail must be used to transmit such data:

**Either**:

Obtain express consent from the Head of School to provide the information by e-mail and exercise caution when sending the e-mail and always follow these checks before releasing the e-mail:

Encrypt and password protect.

Verify the details, including accurate e-mail address, of any intended recipient of the information

Verify (by phoning) the details of a requestor before responding to e-mail requests for information

Do not copy or forward the e-mail to any more recipients than is absolutely necessary

- Do not send the information to any person whose details you have been unable to separately verify (usually by phone)
- Send the information as an encrypted document **attached** to an e-mail
- Provide the encryption key or password by a **separate** contact with the recipient(s)
- Do not identify such information in the subject line of any e-mail
- Request confirmation of safe receipt

**Appendix 3**

**Cyberbullying**
At CAEA we are committed to safeguarding the welfare of all pupils to the best of our ability. We actively invite the participation of parents to help us do this.

We regard pornography/ extremism/ cyberbullying as degrading and exploitive. It can encourage or lead to abusive behaviour, and if pupils are found to have been viewing any type of offensive material at School, the matter will be considered serious and dealt with according to the schools sanctions. (See above)

We oppose the viewing of age-inappropriate films and DVDs. Within the Houses the screening of material is vetted by the Head of Care or Housemaster. Within lessons, subject teachers consult the Head of School or Principal if they wish to use age- inappropriate sources in teaching.

**What is Cyber-bullying?**
Cyber-bullying is the use of Information Communications Technology (ICT), particularly mobile phones and the internet, deliberately to upset or bully someone else.
**Supporting the person being bullied**
Give reassurance that the person has done the right thing by telling someone, refer to any existing pastoral support/procedures and inform parents.

**Advise on next steps:**
1. Make sure the person knows not to retaliate or return the message.
2. Ask the person to think about what information they have in the public domain.
3. Help the person to keep relevant evidence for any investigation (e.g. by not deleting messages they've received, and by taking screen capture shots and noting web addresses of online cyber-bullying instances).
4. Check the person understands simple ways to prevent it from happening again, e.g. by changing contact details, blocking contacts or leaving a chat-room.
5. Take action to contain the incident when content has been circulated:
a) If you know who the person responsible is, ask them to remove the content.
b) Contact the host (e.g. the social networking site) to make a report to get the content taken down.
c) Use disciplinary powers to confiscate phones that are being used to cyber-bully. Ask the pupil to tell you who they have sent messages on to.
d) In cases of illegal content, contact the police, who can determine what needs to be kept for evidential purposes.

**Investigating incidents**
1. All bullying incidents should be properly recorded and investigated.
2. Cyber-bullying can be a very serious matter and can constitute a criminal offence. In UK law, there are criminal laws that can apply in terms of harassment or threatening and menacing communications.
3. Advise pupils to try and keep a record of the bullying as evidence. It can be useful to show parents, teachers, pastoral care staff and the police, if necessary, what has happened.
4. Take steps to identify the bully, including looking at the school systems, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary. The police will need to be involved to enable the service provider to look into the data of another user.

**Working with the bully and sanctions**
Once the person bullying is identified, steps should be taken to change their attitude and behaviour as well as ensuring access to any support that is required. Factors to consider when determining the appropriate sanctions include:
a) The impact on the victim: was the bully acting anonymously, was the material widely circulated and humiliating, how difficult was controlling the spread of the material?
b) The motivation of the bully: was the incident unintentional or retaliation to bullying behaviour from others?
c) Technology-specific sanctions for pupils engaged in cyber-bullying behaviour could include limiting internet access for a period of time.

**Preventing Cyber-bullying**
The best way to deal with cyber-bullying is to prevent it happening in the first place. There is no single solution to the problem of cyber-bullying. These are the five key areas:

**1. Understanding and talking about cyber-bullying**
We all need to be aware of the impact of cyber-bullying and the ways in which it differs from other forms of bullying. Our pupils are made aware of their responsibilities in their use of ICT, from the Internet Access Policy, which also indicates the sanctions for misuse. All students are expected to sign the CAEA Acceptable Use Agreement. Students and parents know that the school can provide them with support if cyber-bullying takes place out of school.

**2. Existing policies and practices**
We review and update the school's anti-bullying policy plus other relevant policies – for example, policies on behaviour, pastoral care and e-learning strategies. We have recently reviewed our existing Acceptable Use Policies (AUPs) – the rules that students have to agree to follow in order to use ICT in school – and publicise them to parents and students. Records are kept of any incidents of cyber-bullying. We are able to conduct searches of internet use records at school, and knowing that the school is taking such steps may act as a disincentive for bullies to misuse school equipment and systems.

**3. Making reporting cyber-bullying easier**
No one should feel that they have to deal with cyber-bullying alone, but reporting any incident of bullying can be really hard for the person being bullied and for bystanders. Notices regarding how to report cases of cyber-bullying are displayed in both Houses.

**4. Promoting the positive use of technology**
Technology at the School is successfully being used to support engaging, positive and effective learning, and to realise and increase the potential of personalised learning by making learning more flexible, creative and accessible. We seek to promote safe ways of using technology with learners to support self-esteem, assertiveness, and participation and to develop friendships. We also discuss 'netiquette', on-line safety and digital literacy.

**5. Evaluating the impact of prevention activities**
Regular reviews are vital to make sure that anti-bullying policies are working and are up-to-date. Once a term we ask one house to complete a questionnaire covering the pupils' experiences of bullying, including cyber-bullying.

**We expect parents:**

*To support the school in its Internet Access and Cyber- bullying policy.
*To try to know your child's online friends as you know their actual friends.
*To ensure that computer use at home is not excessive

***This policy should be read in conjunction with the***

- ***Anti-Bullying Policy***
- ***Safeguarding Policy***
- ***Privacy Notice (Data Protection Policy)***
- ***Data Policies and Procedures***
- ***Data Protection – Data Breach Policy***
- ***Data Protection – Practical Document for Staff***

## Centre Academy East Anglia – ICT Code of Conduct

*To follow the school's 'Acceptable ICT Use Agreement', 'Behaviour', 'E Safety & Data Security' and 'Anti-Bullying Policies.'*

- To only use ICT systems in school, including the internet, email, digital video and mobile technologies for school purposes.
- Not to download or install software on school technology.
- Look after the computer equipment understanding that eating and drinking at the workstations is not permitted.
- Any concerns over ESafety while using electronic communications, such as social media, chatrooms, forums, visiting websites must be reported immediately to the ICT Teacher / ESafety Officer – Mr W.Pipe.
- Not to access sites containing sexualised content or sites linked to terrorist activity that promote extreme views and support violence, further to the school's Prevent Duty and the Counter Terrorism Act 2015. All concerns are to be reported to the Safeguarding– Mrs A. Shaul.
- Any form of online or cyber bullying will not be tolerated.
- Keep your personal information private, do not reveal your passwords to anyone or give out personal information such as your name and address.
- Respect the privacy and ownership of other's work on-line or on the school's computers.
- Images of pupils or staff must never be distributed outside of the school network without permission of all parties involved.
- Any computer games that are played must be of suitable content and within the player age limits, according to the games' PEGI rating.

# 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.

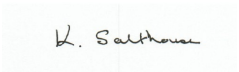
During lessons, teachers will guide students towards appropriate material. Outside of school, families bear the same responsibility for such guidance as they exercise with information sources such as television, telephones, videos, movies, radio and other potentially offensive media.

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.

I would be grateful if you 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.

Yours faithfully,



Mrs K Salthouse
Head of 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**: ……./……../…….

# Centre Academy East Anglia
# 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 any 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**: ...../……/……..

# Centre Academy East Anglia
# Acceptable Use Agreement – Mobile Phones

## Name of Student: Class:

For young people today the ownership of a mobile phone e device is considered a necessary and vital part of their life. When used creatively and responsibly these have great potential to support a student's learning experiences. However, a rise in the number of incidents of misuse of devices in school has created a situation where implementing a specific set of policy guidelines covering mobile phone use in school is deemed necessary.

These guidelines are intended to help make clear the expectations of the school on pupil use of mobile phones and e devices and the restrictions which are placed on their use in school. The guidelines sit alongside the Acceptable use Policy for ICT which all pupils sign. They also give clear guidance to staff, pupils and parents about the consequences for breaches of the Guidelines.

- Pupils will receive age appropriate guidelines and education to help avoid potentially dangerous situations
- All pupils must look after each other and report concerns of misuse or abuse
- All devices should be named and password protected
- Lost/found devices should be taken to the office
- Pupils will be advised to use passwords/pins and to keep these confidential

**Rules for the Acceptable Use of Mobile Phones in school by pupils**

- All pupils must hand in their mobile phones to staff and only use them at the permitted times
- Pupils are not allowed to use mobile phones around school
- Pupils may forfeit the right to have a mobile phone in school if they contravene these guidelines
- Boarding houses have rules about handing in of mobile phones in the evenings. See boarding house handbooks

**Phones and other e-devices**

- No pupil should have age inappropriate material, e.g. videos, games, movies or bring it into school on any of their electronic devices
- No pupil should access age inappropriate material over the internet e.ge. YouTube, Netflix and Love Film
- If asked to so, pupils must show content on the phone (e.g. messages, emails, pictures, videos, sound files ) to a member of staff
- The security of the phone is the pupil's responsibility. It is recommended that all ICT devices are password protected and that pupils change their password regularly ad never reveal it to anyone.

**Dealing with breaches of the Guidelines**

The misuse of the mobile phone devices will be dealt with using the same principles set out in the school behaviour policy, with the response being proportionate to the severity of the misuse. The Principal along with the Head of School will deal with serious incidents of misuse, particularly where there has been a victim of Cyberbullying.

**Unacceptable use**

The school will consider any of the following to be unacceptable use of the mobile phone/e-device and a serious breach of the school's behaviour policy resulting in sanctions being taken.

- It is forbidden to record photographic images (still or video) or sound recordings of staff or pupils without their knowledge and explicit permission
- Photographing or filming in toilets, changing rooms and similar areas is not allowed
- The use of a mobile phone or e-device for 'sexting' (the deliberate taking and sending of provocative images or text messages)
- Bullying, harassing, or intimidating staff or pupils by the use of text, email or multimedia messaging, sending inappropriate messages or posts to social networking or blogging sites. Centre Academy East Anglia will not tolerate cyberbullying
- Making disrespectful comments. We expect pupils to treat other pupils and staff online with the same standards of consideration and good manners as they would in a face to face situation

- General disruption to learning
- Refusing to switch an e-device off or and it over at the request of a member of staff
- Using the mobile phone e-device outside school hours to intimidate or upset staff and pupils will be considered a breach of these guidelines in the same way as unacceptable use which takes place in school time

**Sanctions**
Pupils and parents are notified that appropriate action will be taken against those who are in breach of the acceptable use guidelines. In addition pupils and their parents should be clear that the school is within its rights to confiscate or ban a pupil from having a phone/e-device in school where the guidelines have been breached.

If a phone/e-device is confiscated school will make it clear for how long this will be and the procedure to be followed for its return.

Pupils should be aware that the police will be informed if there is a serious misuse where criminal activity is suspected.

If a pupil commits an act which causes serious harassment, alarm or distress to another pupil or member of staff the ultimate sanction may be permanent exclusion. School will consider the impact on the victim of the act in deciding the sanction and parents will be involved.

The Principle, or Head of School will have the right to view files stored in confiscated equipment and will seek the cooperation of parents in deleting any files which are in clear breach of these Guidelines unless these are being preserved as evidence.

If required evidence of the offence will be preserved, preferably by confiscation of the device and keeping it secure or by taking photographs of the screen.

The Head of School will consider whether an incident should be reported to the DSL.

Following any such incident support will be offered and efforts made to facilitate effective closure for the victim. We also ensure that the perpetrator and any others are educated about the impact of their actions. The Head of School/Principal will document the case history.

**Confiscation Procedure**
If a mobile phone or e-device is confiscated then:

- We will ensure that confiscated equipment is stored in such a way that it is returned to the correct person
- In the case of repeated misuse the phone/e device will be returned and the pupil will lose the right to bring into school

I agree to accept the conditions outlined above:

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

# 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 Jonathan Pipe – 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 only use the approved, secure e-mail system(s) for any school business
- 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 ……