Digital and Online Safety

Approved by:	Last reviewed on:	Next review due by:
Governors	3rd July 2024	July 2025

Contents

1. Aims 2
2. Legislation and guidance 2
3. Roles and responsibilities 3
4. Educating pupils about online safety 5
5. Educating parents/carers about online safety 6
6. Cyber-bullying 6
7. Acceptable use of the internet in school 8
8. Pupils using mobile devices in school 8
9. Staff use of work devices, both inside and outside of school 8
10. Data security and protection 11
11. How the school will respond to issues of misuse 11
12. Training 12
13. Monitoring arrangements 13
14. Links with other policies 13

Appendix 1: KS3 and KS4 acceptable use agreement (pupils and parents/carers) 14

Appendix 2: Acceptable use agreement (staff, governors, and visitors) 15

ADDENDUM: Acceptable Use Policy (AUP) for Remote Learning, including live streamed lessons 18

1. Aims

It is essential that children are safeguarded from potentially harmful and inappropriate online material. The CE Academy takes a whole school approach to online safety in order to protect and educate pupils and staff in the use of technology.

The CE Academy aims to:

- have robust processes in place to ensure the online safety of pupils, staff, and governors;
- Identify and support groups of pupils that are potentially at greater risk of harm online than others;
- deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (mobile phones, smart watches etc);
- 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, antisemitism, 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 scams

2. Legislation and guidance

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

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

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

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

This policy complies with our funding agreement and articles of association.

3. Roles and responsibilities

3.1 The governing board

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

The governing board will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The governing board will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

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

The governing board should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The governing board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting the 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.

The governor who oversees online safety is Gail Brainwood.

All governors will:

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

3.2 The headteacher

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

3.3 The designated safeguarding lead

Details of the school's designated safeguarding lead (DSL) and deputies are set out in our safeguarding and child protection policy.

The DSL takes lead responsibility for online safety at the CE Academy, 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 and governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly.
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks.
- Working with the ICT manager to make sure the appropriate systems and processes are in place.
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents.
- Managing all online safety issues and incidents in line with the school child protection policy.
- Ensuring that any online safety incidents are logged 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.
- Liaising with other agencies and/or external services if necessary.
- Providing reports on safeguarding issues including online safety at the academy to the headteacher and governing board.
- Undertaking annual risk assessments that consider and reflect the risks children face.
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively.

This list is not intended to be exhaustive.

3.4 The ICT manager

The ICT manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material.
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly.
- Conducting a full security check and monitoring the school's ICT systems on at least a termly basis.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.

This list is not intended to be exhaustive.

3.5 All staff

All staff 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 2), and ensuring that pupils follow the school's terms on acceptable use (appendix 1).
- 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.
- Following the correct procedures by if they need to bypass the filtering and monitoring systems for educational purposes.
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'.
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'.
- This list is not intended to be exhaustive.

3.6 Parents/carers

Parents/carers 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/carers can seek further guidance on keeping children safe online from the following organisations and websites:

  What are the issues? – UK Safer Internet Centre
  Hot topics - Childnet
  Parent resource sheet – Childnet

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 2).

4. Educating pupils about online safety

Pupils at the CE Academy will be taught about online safety as part of the curriculum.

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

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

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

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

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

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

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

The CE Academy will use every opportunity, including PACC sessions (PSHE/RSHE, Careers and Citizenship) and social times to raise pupil's awareness of the dangers that can be encountered online.

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

5. Educating parents/carers about online safety

The academy will raise parents/carers' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents/carers on the CE Academy website.

If parents/carers 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.

- Parents/carers are welcome to contact the academy with questions regarding the internet and its use.
- Parents/carers are made aware that pupils will be asked to sign the Acceptable Internet Use Policy Statement before being allowed access to the network.
- Internet issues will be handled sensitively to inform parents/carers without undue alarm.

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 1 person or group by another person or group, where the relationship involves an imbalance of power.

It includes the posting of threatening, abusive, defamatory or humiliating material to social media sites or personal accounts, hijacking of email/social media accounts for malicious use, the misuse of mobile telephones to make threats, send abusive texts or calls, the misuse of mobile phone cameras and associated technology to cause distress, fear or humiliation including using social media to insult, intimidate and spread rumours, all of which detract from our focus on learning.

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 academy will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Staff are encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes PACC (PSHE, Careers and Citizenship), and other subjects where appropriate.

All staff and governors receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 12 for more detail).

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the academy's Behaviour Management policy. Where illegal, inappropriate or harmful material has been spread among pupils, the academy 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 if involves illegal material and will work with external services if deemed necessary.

6.3 Examining electronic devices

The headteacher, and any member of staff authorised to do so by the headteacher can carry out a search and if necessary confiscate any electronic device where they believe is evidence in relation to an offence.

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 and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the senior leadership team (the DSL is a Deputy Head) 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, which may involve handing the device to the Police.

If the material is not suspected to be evidence in relation to an offence, staff members will encourage the pupil and/or the parent 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
- report the incident to the DSL 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 complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

6.4 Artificial intelligence (AI)

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

The CE Academy 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.

The CE Academy will treat any use of AI to bully pupils in line with our anti-bullying and behaviour policies.

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/trust.

7. Acceptable use of the internet in school

All pupils, parents/carers, staff, and governors are expected to sign an agreement regarding the acceptable use of the academy's ICT systems and the internet (appendices 1 and 2). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the academy'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, governors and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate.

CE staff laptops will be subject to random checks to ensure they are being used appropriately.

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

8. Pupils using mobile devices in school

- Pupils are not permitted to use their mobile phones during the school day. This includes mobile phones without SIM cards.
- On arrival 'phones should be put in the 'phone locker and will not be taken out until the end of their school day.
- Recharging 'phone lockers are available for young people.
- Young people can be contacted during the day through the campus office administrator. This is for urgent/emergency messages only.
- If a young person is seen/heard to have 'phones, Bluetooth speakers or wearing headphones/air pods they will be asked to put them in a locker. If they refuse parents/carers will be called.
- If the young person still refuses to put the phone away they may receive an alternative provision on the following campus day.
- After debrief parents/carers will be called again to update them.
- Repeated misuse of the 'phone may result in a longer change of arrangements regarding their timetable.
- The only headphones allowed will be attached to an MP3 player. Pupils will need to show staff the MP3 player is attached to the headphones.
- Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see Appendix 1) and the Mobile Phones Code of Conducts.

9. Staff use of work devices, both inside and outside of school

The use of ICT can enhance teaching and learning. We have put the responsibility on teachers to use this tool in delivering the curriculum and supporting young people. The CE Academy provide laptops for staff to enable them to maximise the potential for using ICT in the classroom.

All staff members will take appropriate steps to ensure their work device (ie laptop) remain safe and 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 (eg asterisk or currency symbol).
- Not sharing the password to their work device with others.
- Not sharing the device among family or friends.

- Not allowing young people to have access to Teacher or Admin accounts.
- Installing anti-virus and anti-spyware software.
- Keeping operating systems up to date by always installing the latest updates.
- Inform and seek advice from the ICT manager if there are any concerns over the security of a loaned work device.

Staff members must not use the device in any way which would violate the academy's terms of acceptable use, as set out in appendix 2. Random checks will be made to ensure this is adhered to. Work devices must be used solely for work activities and are for use in the teaching and learning of CE pupils and professional research by staff to support CE.

Staff laptops remain the property of the CE Academy and can be recalled by SLT at any time.

At home

- In the event of a burglary involving the theft of the equipment, the police must be notified and a Crime Number obtained.
- Staff are asked to check their Home Insurance Policy, as some companies will cover specified business equipment on loan at home at no extra charge.
- The CE Academy is not responsible for any costs incurred through Internet accounts.

In transit

- The CE Academy policy does not cover equipment on loan in transit. Staff should ensure that their Motor Insurance Policy covers them for damage to or theft of business equipment on loan in their car.
- Staff are expected to take reasonable care to ensure the safety and security of equipment on loan while in transit. Equipment should not be left unattended in a vehicle. If this is unavoidable, it must be locked out of sight in the boot.

9.1 Digital Communication

Communication and file sharing is done through Google Workspace and is encrypted by 2 factor authentication. Staff are encouraged to store data on Google Drive. If USB devices are used they must be encrypted.

The academy provides each member of staff and pupil with an email address. The CE Academy use cloud-based email. Staff email accounts should be used for work purposes only.

Staff must take care with the content of all email/text messages and must not use improper language.

Staff must not share their personal phone numbers with parents/carers or pupils.

Staff may use their personal mobile phone/landline for work purposes but must ensure their personal phone number is not detectable by using the correct blocking method for their device. Staff must not use their personal mobile phone to take photographs or videos of pupils.

In some circumstances, it may be appropriate for staff to use their mobile phones for work purposes. Such circumstances may include, but aren't limited to:

- Emergency evacuations
- Supervising off-site visits
- Supervising residential visits

Each campus has a mobile phone which can be used by staff and pupils and can be taken on school trips.

9.2 Social media

Staff are not permitted to access social media websites from the academy's computers or other academy device at any time unless authorised to do so by a member of the Senior Leadership Team. All school devices are monitored.

However, staff may use their own devices to access social media websites outside the school day.

Excessive use of social media, which could be considered to interfere with productivity, will be considered a disciplinary matter.

Staff should assume that anything they write (regardless of their privacy settings) could become public so should ensure that they are professional at all times.

Before joining the academy, new employees should check any information they have posted on social media sites and remove any post that could cause embarrassment or offence.

Any use of social media made in a professional capacity must not:

- Bring the academy into disrepute
- Breach confidentiality
- Breach copyrights of any kind
- Bully, harass or be discriminatory in any way
- Be defamatory or derogatory
- Breach GDPR
- Be used as an alternative to using CE processes and procedures

Whilst we recommend staff do not use social media sites, the academy appreciates that staff may make use of them in a personal capacity. However, staff must be aware that if they are recognised from their profile as being associated with the academy, opinions they express could be considered to reflect the academy's opinions and so could damage the reputation of the school. For this reason, staff should not mention the academy by name, or any member of staff/pupil by name or position.

Those working with children have a duty of care and a statutory duty to report signs of potential radicalisation but also need to be on the lookout for cyber bullying and other activities on social media which might affect the mental health of pupils.

When using social media staff should:

- Never share work log-in details or passwords.
- Keep personal phone numbers private.
- Never give personal email addresses to pupils or parents/carers.
- Restrict access to certain groups of people on their social media sites and pages.
- Regularly update privacy settings.
- Never make 'friends' of pupils at the academy because this could potentially be construed as 'grooming', nor should they accept invitations to become a 'friend' of any pupils.
- Never make 'friends' of ex pupils until they are three years beyond school leaving age.

Staff should keep any communications with pupils transparent and professional and should only use the academy's systems for communications.

If there is any doubt about whether communication between a pupil/parent and member of staff is acceptable and appropriate a member of SLT should be informed so that they can decide how to deal with the situation.

10. Data security and protection

All users of the academy's ICT facilities should set strong passwords for their accounts and keep these passwords secure.

The CE Academy has two filtering systems:

- Device filter - Impero
- Network filter - Surf Protect Quantum (EXA) with automatic blocks

The ICT manager and DSL conducts regular filtering network checks.

2 step authenticator is needed to use Google Workspace and 'Edaware/CPOMS' (Safeguarding reporting system).

Staff and pupils have differentiated internet access.

All personal data is stored in line with data protection regulations and the data protection policy. The Data Protection policy can be found on the academy website.

11. How the school will respond to issues of misuse

Where a pupil misuses the academy's ICT systems or internet, we will follow the procedures set out in this policy and our policies on Behaviour Management and Anti-Bullying. 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 academy'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 this policy and the staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The academy will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police and or Designated Officer (LADO).

All incident types below could be considered criminal in nature or a breach of professional standards. There would be a full investigation in order to determine the outcome.

- Copyright infringement through copying diagrams, texts and photos without acknowledging the source.
- Misuse of logins (using someone else's login)
- Distributing, printing or viewing information on the following:
  - pornography
  - hate material
  - drugs
  - weapons
  - violence
  - racism
- Distributing viruses
- Hacking sites
- Gambling
- Accessing age restricted material
- Bullying of anyone
- Viewing, production, distribution and possession of indecent images of children
- Grooming and harassment of a child or young person

- Viewing, production distribution and possession of extreme pornographic images
- Buying or selling stolen goods
- Inciting religious hatred and acts of terrorism
- Downloading multimedia (music and films) that has copyright attached. (Although this is illegal most police forces would treat this as a lower priority than the cases above.)

Any breach of this policy may lead to disciplinary action under the academy's disciplinary policy. Serious breaches of this policy, such as incidents of bullying or of social media activity causing damage to the organisation, may constitute gross misconduct and lead to dismissal.

Radicalisation

Staff need to be aware that those attempting to groom youngsters for radicalisation are known to work through social media platforms. Any concerns must be reported to SLT and the DSL.

12. 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, newsletters 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 up the risks
- 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.

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

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

13. Monitoring arrangements

The DSL will monitor all incidents relating to online safety through the safeguarding systems in place. All CE staff are trained in the use of Edaware/CPOMS (online recording system). All incidents would be considered to be safeguarding matters and duly recorded, reported and followed up on by relevant staff.

An annual online safety self-review will be conducted using the 360 degree safe tool in order to review practice and policy and to identify strengths and areas for development.

This policy will be reviewed annually by the DSL. At every review, the policy will be shared with the

Governing board. The review will be supported by an online safety audit 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.

14. Links with other policies

This Digital and Online Safety Policy is linked to the following policies:

- Safeguarding and Child Protection
- Behaviour Management
- Anti-Bullying
- Disciplinary Procedures
- Code of Conduct for Staff
- Complaints Policy and Procedure
- Data Protection Policy and Privacy Notices

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

ACCEPTABLE USE OF THE ACADEMY'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Name of pupil:	
When I use the academy's ICT systems (like computers) and get onto the internet in school I will: • Always use the academy's ICT systems and the internet responsibly and for educational purposes only • Only use them when a member of staff is present, or with a member of staff's permission • Keep my usernames and passwords safe and not share these with others • Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of a member of staff or parent/carer • Tell a member of staff immediately if I find any material which might upset, distress or harm me or others **I will not:** • Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless a member of staff has expressly allowed this as part of a learning activity • Use any inappropriate language when communicating online, including in emails • Create, link to or post any material that is pornographic, offensive, obscene or otherwise inappropriate • Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision • Be involved in anything that can attack or corrupt the academy's ICT systems • Use any personal mobile electronic devices (eg phone, Bluetooth speaker) whilst at school **If I bring a mobile phone in to school I will:** • Either hand it in to a member of staff or put it in a locker • Accept that my phone will not be returned until the end of the school day I agree that the school will monitor the websites I visit and may withdraw the right to access the internet if this agreement is not adhered to. The CE Academy reserves the right to examine or delete any files that may be held on its ICT system.	
Signed (pupil):	**Date:**
Parent/carer's agreement: I agree that my child can use the academy's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the academy's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 2: Acceptable use agreement (staff, governors, and visitors)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, AND VISITORS	
Name of staff member/governor/visitor:	
When using the academy's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) • Use them in any way which could harm the school's reputation • Access social networking sites or chat rooms • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software, or connect unauthorised hardware or devices to the academy's network • Share my password with others or log in to the academy's network using someone else's details • Use personal digital cameras or camera phones to take photographs/videos of pupils without checking with SLT first • Share confidential information about the academy, its pupils or staff, or other members of the community • Access, modify or share data I'm not authorised to access, modify or share • Promote private businesses, unless that business is directly related to the school • Use for personal financial gain, gambling or political purposes • Store confidential data on an unencrypted USB drive. • Share personal information like address, personal email address, mobile phone number or landline number with pupils or parents/carers. Staff in each campus has access to a campus mobile phone. • Request or accept invitations from pupils to be 'friends' on social media platforms. There must be a gap of 3 years from when pupils leave the CE Academy (statutory school leaving age) until there is any social media contact between staff and pupils.	
I will only use the academy's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. I agree that the academy will monitor the websites I visit and my use of the academy's ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the academy's ICT systems and internet responsibly, and do my upmost to ensure that pupils in my care do so too.	
Signed (staff member/governor/visitor):	**Date:**

KEY STAGE 3

Mobile Phones

You can bring your phone to school if you follow the

Code of Conduct

You must *hand your phone in on arrival at your campus. It will be returned at the end of your school day.*

In an emergency you can be contacted through the campus secretary.

CONSEQUENCES of not handing in your phone.

If staff see or hear your phone or headphones/airpods:

1. **a warning – you will be asked to hand your phone/headphones to a member of staff;**
2. **if you refuse to hand in your phone/headphones your parents/carers will be called and asked to speak to you;**
3. **if you still refuse to hand in your phone/headphones your parents/carers will be called at the end of the school day, to update them and to ask them to intervene;**
4. **if you refuse again to hand in your phone/headphones you and your parents/carers will be asked to attend a meeting.**
5. **Mobile phones without SIM cards are not acceptable in the campus site.**

The CE Academy is not responsible for your mobile phone whilst it is in the locker.

I understand and agree to the school policy on mobile phones:

Signed (young person).....

A

Mobile Phones (KS4)

You can bring your phone to school if you agree to the following Code of Conduct:

- ✓ On arrival at the campus your mobile phone/headphones/airpods should be handed in and put in a locker. They will not be taken out until the end of your school day.
- ✓ Recharging lockers are available for you to use.
- ✓ Your mobile phone/headphones must not be seen or heard on site throughout your school day.
- ✓ In an emergency you can be contacted through the campus secretary.

If you are seen/heard to have a phone/headphones:

- Staff will encourage you to put your phone in a locker.
- If you refuse, staff will call your parents/carers and ask them to talk to you.
- If you continue to refuse, your parents/carers will be called again at the end of the school day, to update them and ask for their intervention.
- If you refuse to put your phone away again, you and your parents/carers will be asked to attend a meeting.
- The only headphones allowed will be attached to an MP3 player. You will need to show staff that they are not attached to a phone.
- Mobile phones without SIM cards are not acceptable in the campus.
- If you damage anything in an attempt to get your phone back we will report any criminal damage to the Police.

The CE Academy is not responsible for your mobile phone whilst it is in the locker.

I understand and agree to the school policy on mobile phones:

Signed (young person) _____

ADDENDUM:
Acceptable Use Policy (AUP) for Remote Learning, including live streamed lessons

Please read in conjunction with the following policies:

Digital and Online Safety, Safeguarding and Child Protection, Behaviour Management, Code of Conduct for Staff, Data Protection Policy and Privacy Notices.

Leadership Oversight and Approval

- Remote learning will only take place using the Google Workspace (Google Classroom, Google Meet and Google Drive). Google Workspace has been assessed, trialled and approved by the Senior Leadership Team (SLT).
- Google Classroom is intended to be used by staff delivering online lessons to multiple pupils from CE.
- Administration of Google classroom accounts and settings will be done by a member of the SLT and the ICT Manager
- Staff will only use CE Academy accounts with learners and parents/carers.
- Use of any personal accounts to communicate with learners and/or parents/carers is not permitted. Personal accounts are not granted access.
- Live streamed remote lessons will only take place during school hours (9.00am-3.00pm). A member of SLT can "drop into" a virtual lesson.
- All remote lessons will be formally timetabled and approved by SLT. Live streamed remote lessons will only be held with approval and agreement from SLT.
- All staff receive online training and offered extra support if required. Staff are encouraged to practice a live lesson with a colleague before they live stream their lessons to pupils.

Data Protection and Security

- All remote learning and any other online communication will take place in line with current CE Academy processes and procedures as outlined in the Digital and Online Safety Policy and in line with confidentiality expectations outlined in the Data Protection Policy.
- Lessons may be recorded for safeguarding purposes. In these circumstances staff must inform parents/carers and pupils beforehand. All staff must inform a member of SLT if they record a lesson. This recording will be transferred to a shared folder on Drive and then downloaded onto a secure hard drive and kept at County Office. This would be the only copy retained and kept in line with GDPR requirements.
- Only members of the CE Academy community will be given access to CE accounts. Google Suite is a closed system with access only to staff and pupils with a CE account.
- Access to EXA Networks will be managed by the ICT Manager.
- Staff must ensure that their work device is secure and password protected and that they do not share their password with others. Any USB devices containing data relating to the school must be encrypted. All staff have been issued with a pass number protected USB device. If staff have any concerns about the security of their device, they must seek advice from the ICT manager.
- Staff are not permitted to share contact details if emailing multiple parents/carers and or pupils.
- Staff should not share emails or confidential details with pupils/parents/carers.
- CE Academy are responsible for academy infrastructure to ensure the system is as safe and secure as reasonably possible. The ICT manager will oversee this and offer technical support as required.
- Individual devices provided by CE Academy are protected by up to date virus software.

- Parents/carers/pupils when loaning a laptop provided by the CE Academy must sign and adhere to a device loan agreement, detailing expectations.
- Appropriate privacy and safety settings will be used on all devices loaned by CE Academy and they will be installed with appropriate virus software.
- Individual devices loaned to parents/carers for pupils must be password protected with a strong password (at least 8 characters, combination of upper and lower case letters, numbers and special characters. Parents and carers must ensure that a loaned device is not shared among family and friends and must sign a device loan agreement before a device is loaned.
- In some circumstances a device and/or dongle will be loaned to pupils to enable access to remote learning. Where it is not possible for a learner to access online lessons an alternative will be provided.
- All staff have signed an Acceptable Internet Use and Online Safety Agreement.

Session Management

- Staff will record the date and attendance of any sessions held. Behaviour and academic progress will be recorded in the usual way.
- When live streaming with learners:
  - All pupils will have log in details in advance
  - Pupils should never be given control of the video room.
  - Staff have full control of learner's video and audio feeds and can remove pupils from the lesson if the need arises. See later for restrictions on using video feeds.
  - Pupils/parents/carers should not forward or share access links.
  - Staff are able to disable the "chat messaging" function if appropriate.
- Parents/carers are not required to sit in on virtual lessons. Staff should ensure they attend live lessons ahead of pupils and only leave once all pupils have left.

Behaviour Expectations

- Staff will model safe practice and behaviour online as they would in the classroom.
- All participants are expected to behave in line with existing CE Academy policies (Code of Conduct, Digital and Online Safety) This includes:
  - Appropriate language will be used by all attendees.
  - Pupils are not permitted to take screenshots, record or share images during virtual lessons.
  - Accessing inappropriate material such as pornographic, racist or offensive material is strictly forbidden.
- Expectations for behaviour are identical to those in campus and existing procedures will be followed by staff when addressing issues.
- Where the behaviour of a pupil is highly inappropriate they can be removed from the virtual classroom by the teacher. This action should only be taken in the most serious of cases and should be reported to a member of SLT immediately after the lesson has finished.
- When live streaming, staff and pupils are required to:
  - Wear appropriate dress.
  - Use a virtual backdrop for safeguarding purposes. Where this facility is not available it is sufficient to provide a featureless view behind the learner. If this is not possible the learner's video feed will be disabled if there is more than one learner in the lesson.
  - Consider what is on view from their camera. Whilst some objects may constitute deliberate conversation points, you should ensure no private personal information is visible.
- Educational resources will be used or shared in line with our existing teaching and learning policies, taking licensing and copyright into account.

Policy Breaches, Safeguarding and Reporting Concerns

- Any safeguarding concerns will be reported in accordance with the Safeguarding Policy and the usual CE Academy processes and procedures will be followed. Any safeguarding concerns will be reported to SLT and the DSL on the day.
- If inappropriate language or behaviour takes place, participants involved may be removed by staff, the session may be terminated, and concerns will be reported to SLT and/or DSL's.
- Inappropriate online behaviour will be responded to in line with existing policies such as Digital and Online Safety, Safeguarding and Child Protection, Allegations against Staff, Anti-bullying and Behaviour Management.

  Sanctions for deliberate misuse may include:

  - Restricting use
  - Removing use,
  - Contacting police if a criminal offence has been committed.

Policy Control Sheet

Version:	02
Approved by:	Governors
Date approved:	3rd July 2024
Date of next review:	July 2025
Policy Owner:	L Bridger - SLT

Document History			
Version	**Date of review**	**Author**	**Note of revisions**
01	March 2023	L Bridger - SLT	Combination of Acceptable Use of the Internet Policy and Procedures, mobile phone code of conduct and remote learning.
02	June 2024	L Bridger	In line with KCSIE 23 - DSL responsibility to understand filtering and monitoring systems and processes. More details regarding Governing body duties, roles and responsibilities with regards to monitoring and filtering. Addition of AI information Change parents to parents/carers throughout