

Online safety policy

Castle Hall Academy



Approved by:	Date:
Last reviewed on:	November 2020
Next review due by:	November 2021

Castle Hall Academy Online Safety Policy

Contents

- 1. Aims 3
- 2. Legislation and guidance 3
- 3. Roles and responsibilities 3
- 4. Educating pupils about online safety 5
- 5. Educating parents about online safety 6
- 6. Cyber-bullying..... 6
- 7. Acceptable use of the internet in school..... 7
- 8. Pupils using mobile devices in school 7
- 9. Staff using work devices outside school..... 7
- 10. How the school will respond to issues of misuse 7
- 11. Training 7
- 12. Monitoring arrangements 8
- 13. Links with other policies..... 8
- Student Acceptable Use Policy Academy Policy 9
- Acceptable Use Policy Agreement** 9
- Parent / Carer Countersignature**..... 12

Castle Hall Academy Online Safety Policy

1. Aims

Our school aims to:

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

2. Legislation and guidance

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

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

It also refers to the Department's guidance on [protecting children from radicalisation](#).

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

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

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

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3)

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 DSL Sinead Jefferson are set out in our child protection and safeguarding policy as well relevant job descriptions.

Castle Hall Academy Online Safety Policy

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged on CPOMS 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 regular reports on online safety in school to the headteacher and/or governing board

This list is not intended to be exhaustive.

3.4 The ICT manager

The ICT manager is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a 6 monthly 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 on CPOMS and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.5 All staff and volunteers

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

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet, and ensuring that pupils follow the school's terms on acceptable use.
- Working with the DSL to ensure that any online safety incidents are logged on CPOMS 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.

3.6 Parents

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy

Castle Hall Academy Online Safety Policy

- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2)

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

- What are the issues? - [UK Safer Internet Centre](#)
- Hot topics - [Childnet International](#)
- <https://www.net-aware.org.uk/>
- Parent factsheet - [Childnet International](#)

3.7 Visitors and members of the community

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

4. Educating pupils about online safety

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

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**, they 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*

Castle Hall Academy Online Safety Policy

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

The school will use lesson 1 to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

5. Educating parents about online safety

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

Online safety will also be covered during parents' evenings.

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

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

6. Cyber-bullying

6.1 Definition

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

6.2 Preventing and addressing cyber-bullying

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

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Staff will discuss cyber-bullying and the issue will be addressed in lesson one.

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

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

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

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

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

6.3 Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

Castle Hall Academy Online Safety Policy

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on [screening, searching and confiscation](#).

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

7. Acceptable use of the internet in school

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

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

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

More information is set out in the acceptable use agreements.

8. Pupils using mobile devices in school

Pupils may bring mobile devices into school, but are not permitted to use them when on the school site.

Any breach will result in the confiscation of their device.

9. Staff using work devices outside school

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted.

If staff have any concerns over the security of their device, they must seek advice from the ICT manager.

Work devices must be used solely for work activities.

10. How the school will respond to issues of misuse

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

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

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

11. Training

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

Castle Hall Academy Online Safety Policy

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

The DSL [and deputy/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.

Volunteers will receive appropriate training and updates, if applicable.

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

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety

This policy will be reviewed every year by the DSL. At every review, the policy will be shared with the governing board.

13. Links with other policies

This online safety policy is linked to our:

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

Castle Hall Academy Online Safety Policy

Student Acceptable Use Policy Academy Policy

The following is the Academies policy governing the acceptable use of IT Equipment including the Internet and e-mail.

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- that Academy systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

The Academy will try to ensure that students will have good access to digital technologies to enhance their learning and will, in return, expect the students to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use Academy IT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the IT systems and other users.

For my own personal safety:

- I understand that the Academy will monitor my use of the IT systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will be aware of "stranger danger", when I am communicating on-line. I will not arrange to meet them off-line in person.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc)
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the Academy IT system's and devices are primarily intended for educational use and that I will not use them for personal or recreational use.
- I will not make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the Academy IT system's or devices for on-line gaming, on-line gambling, on-line chat, internet shopping, file sharing, audio and video streaming or video broadcasting (eg YouTube) without permission from my teacher.
- I will not change or tamper with Academy IT systems hardware or software nor change any default settings which results in equipment becoming unusable or in need of repair.

Castle Hall Academy Online Safety Policy

- When using any Academy owned portable IT equipment (laptops, netbooks, iPads, digital cameras or smart phones) I understand that it is my responsibility to take care of the equipment whilst in my possession and to be sure it is returned to a teacher in good working order.
 - I understand that in no circumstances should food or drink be consumed when using the Academy IT systems.

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language nor act in a bullying nature and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I recognise that the Academy has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the Academy:

- I will only use my own personal devices (mobile phones / USB devices etc) in the Academy if I have permission to do so. I understand that, if I do use my own devices in the Academy I will follow the rules set out in this agreement, in the same way as if I was using Academy equipment.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others.
- ☒ I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials as stated above.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person / organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will not install or attempt to install or store programmes of any type on any Academy device, nor will I try to alter computer settings.
- I will only use social media sites with permission and at the times that are allowed.

When using the internet within the academy, I recognise that:

- Work/activity/games on the Internet must be directly related to your schoolwork.
- ☒ I should ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

Castle Hall Academy Online Safety Policy

I will be act responsibly in my communications when using the Academy e-mail system:

- I will not send unauthorised transmissions to a third party of confidential material concerning the activities of Castle Hall Academy or infringes the copyright of another person, including intellectual property rights
- I will not allow unauthorised provision of access to Academy services and facilities by third parties
- I will not take part in activities that corrupt or destroy other users' data or that disrupt the work of other users
- I will not take part in the creation or transmission of any offensive, obscene or indecent images, data, or other material, or any data capable of being resolved into obscene or indecent images or material
- I will not send material which is likely to cause annoyance, inconvenience or needless anxiety nor material that is abusive or threatening to others, or serves to harass or bully others
- I will not send material that either discriminates or encourages discrimination on racial or ethnic grounds, or on grounds of gender, sexual orientation, marital status, disability, political or religious beliefs.
- I will not take part in the creation or transmission of anonymous messages, i.e. without clear identification of the sender

I understand that I am responsible for my actions, both in and out of Academy:

- I understand that the Academy also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of Academy and where they involve my membership of the Academy community (examples would be cyber-bullying, use of images or personal information). Please see the BFL policy displayed in all IT classrooms.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This will include loss of access to the Academy network / internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police. Please see the sanctions displayed on the walls in IT classrooms.

Responsibilities of Parents and Carers

- Help and support the school in promoting online safety
- Read, understand and promote the pupil AUP with their children
- Discuss online safety concerns with their children, show an interest in how they are using technology, and encourage them to behave safely and responsibly when using technology
- Consult with the school if they have any concerns about their child's use of technology
- To agree to and sign the home-school agreement which clearly sets out the use of photographic and video images of students.
- To agree to and sign the home-school agreement containing a statement regarding their personal use of social networks in relation the Academy:

We will support the school approach to online safety and not deliberately post comments or upload any images, sounds or text that could upset or offend any member of the school community or bring the school into disrepute.

Castle Hall Academy Online Safety Policy

Please complete the sections on the next page to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to Academy IT systems and devices.

If you do not understand any part of this Acceptable Use Policy, please contact a member of staff.

Student Acceptable Use Policy Agreement Form

This form relates to the Student Acceptable Use Policy, to which it is attached.

Please complete the sections below to show that you have read, understood and agree to the rules included in the Student Acceptable Use Policy. If you do not sign and return this agreement, access will not be granted to Academy IT systems.

I have read and understand the above and agree to follow these guidelines when:

- I use the Academy systems and devices (both in and out of Academy)
- I use my own equipment out of the Academy in a way that is related to me being a member of this Academy e.g. communicating with other members of the Academy, accessing Academy email, VLE, website.

Name of Student

Signed

Date

Parent / Carer Countersignature

I certify that I have read with my child the Castle Hall Academy Student Acceptable Use Policy for use of IT equipment within and outside of the Academy.

Name of Student

Parent Signature

Date

Castle Hall Academy Online Safety Policy

Copyright of the Castle Hall Academy line safety Policy is held by Castle Hall Academy. Any person or organisation wishing to use the document for other purposes should seek consent from Castle Hall Academy and acknowledge its use.

Every reasonable effort has been made to ensure that the information included in this policy is accurate, as at the date of publication in April 2016. However, Castle Hall Academy cannot guarantee its accuracy, nor can it accept liability in respect of the use of the material whether in whole or in part and whether modified or not. Suitable legal / professional advice should be sought if any difficulty arises in respect of any aspect of this new legislation or generally to do with academy conduct or discipline.