CASTLEMAN ACADEMY TRUST

POLICY :

E-Safety

Author:	**Chief Executive Officer**
Date:	**December 2023**
Review Body:	**Trust Board**
Date Adopted:	**6th December, 2023**
Review Date:	**Autumn 2024**
Review Frequency:	**Annual**

Please note that this policy is one of the suite of CAT Policies for School Standards Boards to acknowledge.

CASTLEMAN ACADEMY TRUST
E-SAFETY POLICY

Our policies refer to Senior Leaders. This can mean Executive Head Teacher, Head Teacher or Head of School.

1.Why do we have this policy?

Reason

The Castleman Academy Trust (The Trust) takes its duty to safeguard and promote the well-being of children and young people extremely seriously. In fulfilling this duty the Trust provides a range of education, accommodation and care services including some which use or promote the use of technology. This gives rise to a need to clarify:

a) How staff and volunteers should use technology appropriately in circumstances where contact with young people can occur.
b) How we develop the capacity of children and young people and the adults who work with them to use technology safely and appropriately.

Purpose

To enable children, young people, staff and volunteers to interact with, and benefit from, information technology whilst remaining safe and behaving lawfully.

2. Who must comply with the policy?

All staff and volunteers who work in contact with young people must comply with this policy. Contact means face-to-face contact and remote contact through technology.

Furthermore staff who construct contracts with outside agencies for the provision of services involving contact with children & young people must ensure that the measures described in this policy are included in any contractual arrangements.

3. When does this policy apply?

This policy applies at all times and relates to all work with children and young people and their parents / carers.

4. What is the policy?

Principles

4.1 Staff employed by the Trust to work with children and young people are in a position of trust. They must avoid any conduct which would lead any reasonable person to question their motivation and intentions, and work according to the Government 'Guidance for safer working practice for adults who work with children and young people (2009)' https://pandorsetscb.proceduresonline.com

Staff and volunteers who work with children and young people are able to use the internet, and related communications and technologies, appropriately and safely.

To do this the Trust will:

- Promote and procure technology that helps to support safe and legal working
- Train staff appropriately
- Regulate staff activity
- All staff will work closely with the Designated Safeguarding professional and managers/leadership team to promote E safety and respond to any safeguarding issues

4.2 The Trust believes that all children and young people should be empowered to access appropriate information via technology to develop their learning, support communication and facilitate social interaction.

To do this the Trust will:

- Promote learning about safe and legal use of technology for children and young people plus their parents and carers

4.3 The Trust expects that where staff may have concerns about inappropriate use of technology involving children and young people they must report this immediately and confidentially directly to their line manager/the DSL in accordance with the normal child protection procedures and/or whistle blowing procedures.

To do this the Trust will:

- Operate clear procedures for handling safeguarding incidents involving technology in accordance with national guidance and Safeguarding Children Partnership and Human Resources policies and procedures (see 11 below)
- Train managers accordingly

5. Communication from staff/volunteers to young service users

Communication with children and young people involving digital technology must be carried out in a professional rather than private context. This means that:

i. The communication will be carried out using Trust/school-controlled systems and accounts rather than private ones. Where publically available platforms are used (such as social media services) specific accounts must be setup for official purposes and only with line manager approval. Privacy settings for these should be configured such that identities, personal information and the ability to make unsolicited contact are secured.

ii. Any use of personal devices for professional purposes must be with the agreement of line managers. Staff must consent for managers to have access to such devices (including any access credentials) for routine monitoring purposes. They must agree to any security systems and accept the risk that if misused, it may adversely affect their personal data.

iii. These systems and accounts must be configured such that managers can monitor communications through logs, administration accounts, etc. Managers must carry out monitoring of these accounts both routinely and where there is specific cause for concern.

iv. The content of communications will relate solely to official matters such as learning, impartial advice and guidance, pastoral support or handling practical arrangements for official activities. Any form of communication will be with the knowledge and consent of the parent/carer.

v. Staff/volunteers should take care in their communications with children so as to avoid any possible misinterpretation of their motives or any behaviour which could be construed as grooming

vi. There is strictly to be no contact with any child, young person or any other service user via the professional's personal use of social media sites e.g. Facebook or personal communication systems e.g texting on mobile phone. The only exception is if there is a practical reason to have contact with a young person via a social media site e.g. for a pastoral worker or social worker to befriend a looked after young person on Facebook to monitor their use of this facility. Wherever possible this would be on an account set up specifically for this reason. Permission must be agreed and recorded as part of a care plan and monitored by a manager.

vii. Staff/volunteers - Personal information such as private contact details including phone numbers and social media accounts must not be shared with service users.

viii. Staff/volunteers should not request personal information from children and young people / parents and carers other than that which is required for official purposes and must always be done through official channels.

ix. Where staff breach the restrictions imposed by filtering or other safety mechanisms this is deemed a disciplinary matter.

x. Issues relating to data protection are not covered by this policy but staff must ensure that they are working within appropriate policies in relation to their interactions with children, young people and other service users.

The scope of "communication" includes still and moving images / graphics / audio content as well as text.

6. The use of digital images

i. Written permission from parents or carers must be obtained where digital images are to be made of their children / young people or biometrics are to be gathered for official purposes.

ii. Permission must also be sought from young people where they are of an age to give this.

iii. Care must be taken when capturing digital images that young people are appropriately dressed and are not participating in activities that might bring the individuals or the setting into disrepute.

iv. Photographs should always be taken in a public space, especially where there is only one subject.

v. The full names of young people will not be used anywhere on a website, blog, or published article, particularly in association with photographs. Consideration should be given to media coverage and journalists should be made aware of this policy.

vi. Images must only be made and stored using professional equipment or that approved and secured via the Trust/school.

vii. If the printing of images is to take place away from the setting where the child/young person attends, parents must be made aware of where they will be printed and have given permission for this.

7. Access to Inappropriate Images and Internet Usage

i. There are no circumstances that will justify adults possessing indecent images of children. Adults who access and possess links to such websites will be viewed as a significant and potential threat to children. Accessing, making and storing indecent images of children on the internet is illegal. This will lead to criminal investigation and the individual being barred from working with children and young people, if proven.

ii. Adults should not use equipment belonging to the Trust/School to access adult pornography; neither should personal equipment containing these images or links to them be brought into the workplace.

iii. Adults should ensure that children and young people are not exposed to any inappropriate images or web links. Schools and adults need to ensure that internet equipment used by children have the appropriate controls with regards to access. e.g. personal passwords should be kept confidential.

iv. Where indecent images of children or other unsuitable material are found, the police and Local Authority Designated Officer (LADO) should be immediately informed. Staff or volunteers should not attempt to investigate the matter or evaluate the material themselves, as this may lead to evidence being contaminated which in itself can lead to a criminal prosecution. For Managing allegations against professionals guidance refer to the Department for Education document Keeping Children Safe in Education – part 4.

8. Staff/volunteers private use of digital media

i. In their private use of digital media (such as social networking sites) staff must protect their professional reputation and that of other Trust staff and staff in partner organisations. This must be achieved either through the judicious application of privacy settings so that communications remain private from children and young people / parents and carers and through the avoidance of rhetoric that might cause reputational damage.

ii. Staff/volunteers must not solicit or accept “friend / contact / circle / follow” type connections to private accounts with children and young people for whom they have any professional responsibility.

iii. Staff/volunteers must not engage in any communication which could bring the Trust/school into disrepute which includes postings made on personal sites, blogs in staff’s own time. Staff must be mindful of confidentiality and data protection. If a staff member becomes aware that they have posted a comment which may bring the Trust into disrepute or breach data protection they must bring this to the attention of their manager urgently, who in turn will seek advice from the Senior Leaders. The Trust’s HR Director or provider may get involved after that if the manager needs help to deal with the individual’s behaviour and its impact via the Disciplinary Procedures.

iv. At all times staff must be respectful of others, not engaging in any communication which could be deemed as breaking the law regarding discrimination or offensive behaviour. They must never use

social media to bully or harass another employee, manager or service user including any child or young person.

9. Children and Young people's use of technology

i. Staff who directly supervise children and young people must ensure that use of the Internet through official infrastructure is supervised and / or monitored. The level of this supervision / monitoring should be locally determined based on age, nature of the systems used, nature of the setting, etc. All staff who directly supervise children and young people in the use of technology, must be in receipt of e-safety training which highlights risks and appropriate countermeasures.

ii. Age appropriate safety mechanisms such as content filtering must be employed where children and young people access the Internet through the Trust/school infrastructure. Breaches of these safety mechanisms by children and young people (for example through the use of proxy websites) must always be challenged in an age appropriate way.

iii. Staff must ensure that any films or material they show to children or sites they ask children to access to find information are age appropriate.

iv. It is the responsibility of staff to ensure as far as possible that young people are not, while in their direct care, involved in plagiarism and copyright infringement, illegal downloading of copyright files, hacking, viruses or other breaches of system security.

v. All staff in contact with children and young people have a responsibility to advise about and encourage E safety and good behaviour in relation to personal online activity as well as that in the setting e.g. avoiding contact with strangers which may lead to grooming, access of age appropriate data, use of privacy settings in social media, risks of on-line gaming, cyber bullying, respect for copyright and the security of personal information. Where appropriate this should be through a planned curriculum i.e. digital literacy and E safety. They should advise against excessive use which impacts on social and emotional development.

vi. Even where contact is brief, informal and unstructured, good behaviours should be acknowledged and inappropriate behaviours challenged.

vii. Where a planned curriculum is being delivered this should include some involvement of and advice to parents and carers.

viii. The Trust will ensure there are policies and procedures in place for the safe use of technology, ideally designed in dialogue with those whom it will affect. These will be shared and routinely refreshed through posters, lessons, pastoral work, staff training and induction procedures, etc. They must also be shared with parents and carers.

ix. Acceptable User Policies must be signed by children, young people and where appropriate, their parents/carers and regularly reviewed and up-dated (see South west Grid web site for model AUP www.swgfl.org.uk).

x. Any form of bullying including cyber bullying is not acceptable and there will be sanctions in place for any young person who is engaging in cyber bullying. These will be in the form of an Anti-bullying and/or behaviour policy in schools. For significant events or concerns the Safer Schools and Communities team should be involved.

10. Enforcement

Breaches of this policy will fall into the following categories:

- Illegal acts by staff – Escalated to Police/LADOs/Children's Social Care

- Breaches of policy – Following investigation by LADOs / Children's Social Care/HR/Data protection as appropriate, these are handled by line managers in accordance with the standard disciplinary procedures.

11. Other relevant Guidance

Trust Social Networking Policy

Email and internet policy and other ICT and corporate security policies
Dignity at work
Code of Conduct
Disciplinary procedure

12. Supporting information

Please note that these links are not necessarily kept up to date by the Trust. They are included for information and understanding purposes only and may not reflect current legislation. However, the principles and advice contained within them may be useful. Always liaise with the School's Designated Safeguarding Lead before taking action on the school's behalf.

http://ceop.police.uk/ For advice and guidance from the Police's Child Exploitation and Online Protection Unit (CEOP)

https://swgfl.org.uk/online-safety/ For e-safety support material from the South West Grid for Learning who provide Internet connectivity to nearly all state schools in the 15 South West local authorities as well as actively managed filtering and monitoring. This includes Standard Acceptable User Policies, bring your own device, advice on clouding etc.

http://www.iwf.org.uk/ Internet Watch Foundation for the reporting of criminal online content.

https://www.gov.uk/data-protection/the-data-protection-act Data Protection Act 1998

http://webarchive.nationalarchives.gov.uk/20130401151715/https://www.education.gov.uk/publications/eOrderingDownload/DCSF-00334-2008.pdf Byron review 'Safer children in a digital world'

https://webarchive.nationalarchives.gov.uk/ukgwa/20141107033803/http://www.ofsted.gov.uk/resources/safe-use-of-new-technologies Safe use of new technologies Ofsted 2009

www.education.gov.uk/ukccis Advice on Child Internet Safety 1.0 UK Council for Child Internet Safety

http://www.ico.org.uk/ Data Protection/Information Commissioner's Office (ICO)

Safe Schools and Communities team https://www.dorset.police.uk/help-advice-crime-prevention/safety-in-your-community/ssct/ 01202 222844 . This team provides support if an E safety incident occurs as well as training packages for children, young people, parents/carers and staff.

Equality Impact Assessment

This policy has been reviewed with the equality impact considerations as laid down in the school's Equality Policy.