CASTLEMAN ACADEMY TRUST

POLICY :

Digital Working

Author:	**Strategic IT Lead**
Date:	**December 2024**
Review Body:	**Trust Board**
Date Adopted:	**11th December 2024**
Review Date:	**Autumn 2025**
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

Digital Working Policy

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

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 digital technology. This gives rise to a need to clarify:

- How staff and volunteers should use digital technology appropriately.
- How we develop the capacity of children and young people and the adults who work with them to use digital technology safely and appropriately.

All working with digital systems – teachers, support staff, volunteers and pupils – must be aware of the content of this policy. Contact may mean face-to-face contact and remote contact through digital technology.

All staff and volunteers in the Castleman Academy Trust must adhere to the principles and policy in this document when using digital systems. Teachers will ensure that they have covered these principles in their planning and in the work done by learners

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

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

PURPOSE

The purpose of this policy is to ensure that all stakeholders (Staff, Pupils, Governors and Trust Board members) of Castleman Academy Trust Schools understand the way in which digital technology should be used in and out of school. It aims to ensure that digital technology is used efficiently, securely and safely for the intended purpose without infringing legal requirements.

New technologies are an integral part of our lives and are powerful tools which open up teaching and learning opportunities for school staff in many ways. This document aims to;

- Assist school staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice;
- Set clear expectations of behaviour and/or codes of practice relevant to social networking for educational, personal or recreational use;
- Give a clear message that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken;
- Support safer working practice;
- Minimise the risk of misplaced or malicious allegations made against adults who work with pupils;
- Reduce the incidence of positions of trust being abused or misused.

Whilst every attempt has been made to cover a wide range of situations, it is recognised that this policy cannot cover all eventualities. There may be times when professional judgements are made in situations not covered by this document, or which directly contravene the standards outlined in this document. It is expected that in these circumstances staff in schools will always advise their Senior Leaders of the justification for any such action already taken or proposed. The Senior Leaders will in turn seek advice from the Trust's HR and IT staff where appropriate.

This policy takes account of employment legislation and best practice guidelines in relation to the use of digital technology in addition to the legal obligations of employers and the relevant legislation listed at appendix A.

SCOPE

All staff, pupils, governors, trustees and members (from hereon named "Users") in Castleman Academy Trust Schools, including part-time staff and pupils, are subject to this policy. Failure to comply with the policy may lead to disciplinary action, including suspension/exclusion. At the same time, their conduct and/or action(s) may be in contravention of the law and they may be personally liable.

This policy should not be used to address issues where other policies and procedures exist to deal with them. For example, any alleged misconduct which falls within the scope of the Allegations Against Staff Policy requires the school to comply with additional child protection requirements as set out in that policy.

This document does not replace or take priority over advice given by the Trust's HR or IT staff or the Trust's codes of conduct, dealing with allegations of abuse, other policies issued around safeguarding or IT issues (e.g. data protection policies), but is intended to both supplement and complement any such documents.

PRINCIPLES

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 (2019)' https://pandorsetscb.proceduresonline.com

Adults who work with pupils are responsible for their own actions and behaviour and should avoid any conduct which would lead any reasonable person to question their motivation and intentions.

Staff in schools should work and be seen to work, in an open and transparent way.

Staff in schools should continually monitor and review their practice in terms of the continually evolving world of digital technology and ensure they follow the guidance contained in this document.

Staff and volunteers who work with children and young people should be 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

- Ensure staff work will work closely with the Designated Safeguarding professional and managers/leadership team to promote E-safety and respond to any safeguarding issues

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

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

SECTION 1 : GENERAL DIGITAL WORKING

All school resources, including computers, Email and voicemail are provided primarily for educational purposes of the school and for carrying out activities consistent with their education.

Incidental and occasional personal use of these systems is permitted, subject to the restrictions contained in this policy and with the approval of the Senior Leaders. Any personal use of the Internet or Email is expected to be in staff and student's own time and is not to interfere with lesson time or day to day duties.

Users should not engage in any activity which is illegal, likely to cause offence or have negative repercussions for the Trust and the user's own school. Equipment must not be used to upload, download, use, retain, distribute or disseminate any images, text, materials or software which:

- are or might be considered to be indecent or obscene;
- are or might be offensive or abusive in that its content is or can be considered to be a personal attack, rude or personally critical, sexist, racist, or generally distasteful;
- encourage or promote activities which would, if conducted, be illegal or unlawful;
- involve activities outside those which serve only an educational purpose – for example, unauthorised selling/advertising of goods and services;
- might affect or have the potential to affect the performance of, damage, overload or compromise the Trust's or school's system, network and/or external communications in any way;
- might be defamatory or incur liability on the part of the trust or the school or adversely impact on the image of the trust or the school.

Users should be aware of any potential copyright infringement.

Protection of Personal Information

Staff should never share their work log-ins or passwords with any other people.

Staff should ensure that they use strong passwords for any school accounts. Predictable passwords should be avoided, such as dates, family and pet names. Staff should avoid the most common passwords that criminals can easily guess such as 'passw0rd'. Staff should not re-use the same password across important accounts, if one password is stolen, the criminal can also gain access to, for example, bank accounts.

Passwords should be at least 8 characters long and contain uppercase characters, lowercase characters and symbols.

To create a memorable password that is also hard for someone else to guess, good practice suggests combining three random words to create a single password e.g. Upfish!biRd

Staff should not give their personal e-mail addresses to pupils or parents. Where there is a need for homework to be sent electronically, the school email address should be used.

The Use of Digital Images

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.

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

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.

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

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.

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

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.

Access to Inappropriate Images and Internet Usage

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.

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. This will raise serious concerns about the suitability of the adult to continue to work with children.

Adults should ensure that children and young people are not exposed to any inappropriate images or web links.

Where indecent images of children 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.

Where other unsuitable material is found, which may not be illegal but which raises concerns about that member of staff, either the Trust's HR and Operations Director or the LADO should be informed and advice sought. Schools should refer to the Allegations Against Staff Policy and should not attempt to investigate or evaluate the material themselves until such advice is received.

Children and Young People's Use of Technology

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.

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.

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.

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.

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.

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

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.

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).

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.

SECTION 2 : ELECTRONIC COMMUNICATION

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

Use of Written Communications

Care should be taken when using written electronic communications, including, but not limited to, email, text messaging, Teams, Governorhub, Facebook, X (Twitter), Weduc, ReachMoreParents, Parentmail. Such messages are perceived to be less formal than paper-based communication and there is a tendency to be lax about their content. Users should be aware that written communication, in whatever form, can be easily misunderstood or misinterpreted. Users should bear in mind that they and the Trust will be held accountable for all expressions of fact, intention and opinion they communicate via electronic communications, in the same way as verbal and written paper-based expressions or statements.

It is advised that staff should check with their line manager to ensure they are sending data and information in an appropriate fashion and in line with this policy and the email etiquette guidance at Appendix 1.

Users should not include anything in an electronic communication which they cannot, or are not prepared to, account for. They should not make any statements on their own behalf or on behalf of their school or the Trust which may be considered defamatory or in any way damaging to the reputation of any person or entity.

Electronic messages which have been deleted from the school's system can be traced and retrieved. Therefore, all persons having a part in creating or forwarding any offending electronic message can be identified. Electronic messages, both in hard copy and electronic form, are admissible in a court of law.

Email correspondence can be viewed by others and can become the basis of an enquiry when complaints are received and may form part of a Subject Access Request (SAR).

Care must be taken in the distribution of electronic messages to ensure that they are only be sent to those who need to be aware of the content. "Blanket messages" eg. "All at Castleman Academy Trust Schools" should be used sparingly and NOT for sending messages that are not relevant to the everyone who will receive the email.

Using 'reply all' should not be used in most cases if the information is only relevant to the original sender.

Where email is used to send messages to multiple parents, it is essential that the parental emails are only ever placed in the 'BCC' field.

Care must be taken when 'forwarding' emails to ensure that previous emails in the 'thread', which are not intended for the final recipient, are not disclosed by mistake.

Electronic communications should not be used to communicate personal opinions about pupils, parents, staff, governors etc. If the communication is deemed necessary, it should refer to subjects using initials where possible.

All staff should be vigilant to the possibility of receiving electronic communications that may contain dangerous content or attachments designed to compromise the IT systems or obtain sensitive information. Staff are required to report any such communication or possible breaches to the Trust IT team without delay.

Communication from Staff/Volunteers

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

The communication will be carried out using Trust/school-controlled systems and accounts rather than private ones. It is the expectation that the school should provide a work e-mail address for communication between staff and pupils or parents.

Where publicly available platforms are used (such as social media services) specific accounts must be setup for official purposes and only with the approval of the (Executive) Headteacher. Privacy settings for these should be configured such that identities, personal information and the ability to make unsolicited contact are secured.

Any use of personal devices for professional purposes must be with the agreement of the (Executive) Headteacher. Staff must consent for Trust IT staff 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.

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

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 with a pupil will be with the knowledge and consent of the parent/carer.

Communication With Pupils

Communication between pupils and staff, by whatever method, should take place within clear and explicit professional boundaries. This includes the wider use of technology such as mobile phones, text messaging, e-mails, digital cameras, videos, web-cams, websites and blogs.

Staff should ensure that all communications are transparent and open to scrutiny. They should also be circumspect in their communications with pupils so as to avoid any possible misinterpretation of their motives or any behaviour which could be construed as ‘grooming’ in the context of sexual offending.

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. 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 Trust IT Staff.

Staff/volunteers should not give their personal contact details to pupils including e-mail, home or mobile telephone numbers, unless the need to do so is agreed with senior management and parents/carers.

Staff/volunteers should not request, or respond to, any personal information from a pupil, other than that which might be appropriate as part of their professional role.

E-mail or text communications between an adult and a pupil outside agreed protocols may lead to disciplinary and/or criminal investigations. This also includes communications through internet-based websites. Internal communication systems should only be used in accordance with the Trust's Electronic Communications Policy.

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, staff and volunteers.

Staff Cyberbullying

Cyberbullying can be defined as 'the use of modern communication technologies to embarrass, humiliate, threaten or intimidate an individual in the attempt to gain power and control over them.'

Prevention activities are key to ensuring that staff are protected from the potential threat of cyberbullying. All employees are reminded of the need to protect themselves from the potential threat of cyberbullying. Following the advice contained in this guidance should reduce the risk of personal information falling into the wrong hands.

If cyberbullying does take place, employees should keep records of the abuse, text, e-mails, website or instant message and should not delete texts or e-mails. Employees are advised to take screen prints of messages or web pages and be careful to record the time, date and place of the site.

Staff may wish to seek the support of their trade union or professional association representatives or another colleague to support them through the process. Employees will also have access to a staff counsellor, subject to funding being agreed.

Staff are encouraged to report all incidents of cyberbullying to their (Executive) Head Teacher. All such incidents will be taken seriously and will be dealt with in consideration of the wishes of the person who has reported the incident. It is for the individual who is being bullied to decide whether they wish to report the actions to the police.

SECTION 3 : SOCIAL NETWORKS AND SAFER SOCIAL MEDIA PRACTICE

Objectives

This section sets out Castleman Academy Trust's (CAT) policy on social networking. New technologies are an integral part of our lives and are powerful tools which open up teaching and learning opportunities for school staff in many ways. This document aims to;

- Assist school staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice;
- Set clear expectations of behaviour and/or codes of practice relevant to social networking for educational, personal or recreational use;
- Give a clear message that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken;
- Support safer working practice;
- Minimise the risk of misplaced or malicious allegations made against adults who work with pupils;
- Reduce the incidence of positions of trust being abused or misused.

Whilst every attempt has been made to cover a wide range of situations, it is recognised that this policy cannot cover all eventualities. There may be times when professional judgements are made in situations not covered by this document, or which directly contravene the standards outlined in this document. It is expected that in these circumstances staff in schools will always advise their Senior Leaders of the justification for any such action already taken or proposed. The Senior Leaders will in turn seek advice from the Trust's HR and IT staff where appropriate.

This policy takes account of employment legislation and best practice guidelines in relation to social networking in addition to the legal obligations of employers and the relevant legislation listed at appendix A.

What Is Social Media

For the purpose of this policy, social media is the term commonly used for websites or applications (apps) which allow people to interact with each other in some way – by sharing information, opinions, knowledge and interests. Social networking websites such as Facebook, are well-known examples of social media but the term also covers other web/cloud-based services such as blogs, video and audio podcasts, wikis, message boards, photo document and video sharing websites such as YouTube and micro blogging services such as the site formerly known as Twitter. This definition of social media is not exhaustive as technology develops with new ways of communicating advancing every day. Social media also applies to the use of communication technologies such as mobile phones, cameras or other handheld devices and any other emerging forms of communications technologies.

Overview and Expectations

All adults working with pupils have a responsibility to maintain public confidence in their ability to safeguard the welfare and best interests of pupils. It is therefore expected that they will adopt high standards of personal conduct in order to maintain the confidence and respect of their colleagues, pupils or students, public in general and all those with whom they work in line with the trust's code of conduct. Adults in contact with pupils should therefore understand and be aware that safe practice **also involves using judgement and integrity about behaviours in places other than the work setting.**

The guidance contained in this policy is an attempt to identify what behaviours are expected of all school staff. Anyone whose practice deviates from this document and/or their professional or employment-related code of conduct may bring into question their suitability to work with children and young people and may result in disciplinary action being taken against them.

School staff should always maintain appropriate professional boundaries and avoid behaviour, during their use of the internet and other communication technologies, which might be misinterpreted by others. They should report and record any incident with this potential.

Staff/Volunteers' Private Use of Digital Media

Managing personal information effectively makes it far less likely that information will be misused.

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.

In their own interests, staff need to be aware of the dangers of putting personal information onto social networking sites, such as addresses, home and mobile phone numbers. This will avoid the potential for pupils or their families or friends having access to staff outside of the school environment. It also reduces the potential for identity theft by third parties.

All staff, particularly new staff, should review their social networking sites when they join the school to ensure that information available publicly about them is accurate and appropriate. This includes any photographs that may cause embarrassment to themselves and the school if they are published outside of the site.

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.

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.

Staff should never use or access social networking sites of pupils and should never accept an invitation to ‘friend’ a pupil.

Confidentiality needs to be considered at all times. Social networking sites have the potential to discuss inappropriate information and employees need to ensure that they do not put any confidential information on social media about themselves, their employer, their colleagues, pupils or members of the public.

Employees need to ensure that when they are communicating about others, even outside of work, that they give due regard to the potential for defamation of character. Making allegations on social networking sites (even in their own time and in their own homes) about other employees, pupils or other individuals connected with the school, or another school, could result in formal action being taken against them.

Staff are also reminded that they must comply with the requirements of equalities legislation in their on-line communications.

Staff/volunteers must not engage in any communication which could bring the Trust/school into disrepute which includes postings made on personal social media 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 and Operations Director or HR provider may get involved after that if the senior leader needs support to deal with the individual's behaviour and its impact via the Disciplinary Procedures.

Some social networking sites and other web-based sites have fields in the user profile for job title etc. If you are an employee of a school and particularly if you are a teacher, you should not put any information onto the site that could identify either your profession or the school where you work, which would then bring the school into disrepute. In some circumstances this could damage the reputation of the school, the profession or the Trust.

Social Contact

Staff should not establish or seek to establish social contact via social media / other communication technologies with pupils for the purpose of securing a friendship or to pursue or strengthen a relationship.

There will be occasions when there are social contacts between pupils and staff, where for example the parent and teacher are part of the same social circle. These contacts however, will be easily recognised and openly acknowledged.

There must be awareness on the part of those working with pupils that some social networking contacts, especially where these are not common knowledge, can be misconstrued as being part of a grooming process. This can also apply to social networking contacts made through outside interests or through the staff member's own family.

SECTION 4 : MONITORING

All Castleman Academy Trust resources, including computers, email, Teams and voicemail are provided for school purposes.

At any time and without prior notice, the Castleman Academy Trust and/or the school maintains the right to examine any systems and inspect and review any and all data recorded in those systems. Any information stored on a computer or digital platform, whether the information is contained on a hard drive, computer disk, the cloud or in any other manner, may be subject to scrutiny by the Trust or the school. This monitoring helps to ensure compliance with internal policies, supports the performance of internal investigations, and assists the management of information systems.

SECTION 5 : ENFORCEMENT

All employees must adhere to, and apply, the principles of this policy in all aspects of their work.

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 senior leaders in accordance with the standard disciplinary procedures.

SECTION 6 : LINKS WITH OTHER POLICIES

Policy / Document	Relevance
Allegations Against Staff and Disciplinary Policy and Procedure	Use of social networking sites which is not in accordance with this policy or the Trust's policies may amount to misconduct or gross misconduct under the Trust's disciplinary policy and procedure.
Dignity at Work Policy	Where use of social networking sites can be interpreted to constitute a form of bullying or harassment of another member of staff this may be dealt with under the Fairness and Dignity at Work Policy in the first instance.
Equalities Policy	Use of social networking sites should be at all times in accordance with the school's equal opportunities in employment policy.
Code of Conduct and Guidelines for Safe Working Practices for the Protection of Children and Staff ***Volunteer Code of Conduct*** ***Code of Conduct for Trustees and Governors***	The code sets out the standards of conduct expected of employees including maintaining the school's reputation, non-disclosure of confidential information and standards of behaviour expected.

Section 7 : REVIEW OF POLICY

Due to the ever-changing nature of information and communication technologies it is best practice that this policy be reviewed annually and, if necessary, more frequently in response to any significant new developments in the use of technologies, new threats to e-safety or incidents that have taken place.

Equality Impact

The Trust does all it can to ensure that its policies do not discriminate against pupils or others, either directly or indirectly, in line with any Equality Act 2010 protected characteristics.

Castleman Academy Trust
Email Etiquette

Appendix 1

In order to promote professionalism, effective and efficient working practices, an email code of conduct is vital.

These guidelines are intended to ensure the highest standards of professionalism within our Trust and its schools.

Electronic communication should be:-

✓ Respectful ✓ Appropriate ✓ Understandable ✓ Precise ✓ Accurate

There should be no scope for misunderstanding

Email correspondence can be viewed by others and can become the basis of an enquiry when complaints are received and may form part of a Subject Access Request (SAR).

The points below form the basic principles to which you should adhere to:-

- Is the email the most appropriate form of communication?
- Is the email necessary?
- Are you sending the email to the most appropriate group or individual?
- Can the information be found elsewhere e.g. school website?

Sending an email and email content:-

- Use proper spelling, grammar and punctuation
- Avoid the use of 'text' speak
- Use an appropriate greeting, using the recipient's name
- End the email in an appropriate manner e.g. Kind regards. Do not use less formal and more personal associations e.g. kisses and smiley faces
- Consider the tone of the email, especially if you are requesting help
- Attach files only where necessary
- Use proper structure and layout and include the message subject
- Be concise and to the point
- Do not write in CAPITALS
- Do not send an email when annoyed
- Do not use sarcasm, jokes, insulting or offensive remarks
- Read the email before you send it and reconsider the tone, length and content
- Do not use circulation lists if all recipients do not need to receive the email

Replying to an email:

- Use the following functions carefully and with caution
  - Reply to all
  - Delivery and read receipts
  - 'Urgent' and 'Important'
  - Is it appropriate to use cc
- Do not copy a message or attachment without permission as this may have GDPR implications
- Answer all questions and pre-empt further questions
- Do not use email communication to discuss confidential information
- Be careful when forwarding emails with a long thread as they may have inappropriate text further down which was not intended for the final recipient
- Do not expect a response immediately or out of working hours
- Consider carefully whether an email requires a response, i.e. is only 'thanks' required

APPENDIX 2 : KEY POINTS
Principles

- Adults who work with pupils are responsible for their own actions and behaviour and should avoid any conduct which would lead any reasonable person to question their motivation and intentions.
- Staff in schools should work and be seen to work, in an open and transparent way.
- Staff in schools should continually monitor and review their practice in terms of the continually evolving world of social networking and ensure they follow the guidance contained in this document.

All staff should:

- Use digital communications in line with trust policy.
- Review all personal social networking sites so that no personal information is available to pupils.
- Never "friend" a pupil or past pupil (unless they have attained the age of 18 and have no siblings in the school).
- Restrict (**set privacy to highest settings**) who can see their pages (most social networking sites default to a fairly open setting meaning most people can see their site).
- Remove photos which might be embarrassing to the school or Trust.
- Never make allegations (defamation of character) on social networking sites (even in their own time or from their own computer) about other employees, pupils, other individuals connected with the school or another school.
- Have due regard to equalities legislation when using social networking sites.
- Never post derogatory remarks or offensive comments on line.
- Not use their own equipment for school work e.g. using own camera or own mobile phone.
- Only use work email addresses with parents and pupils.
- Not communicate using school ICT facilities with adults or pupils outside agreed protocols. This may lead to disciplinary or criminal investigation. This includes communications through internet-based websites.
- Not put information onto social networking sites which would identify their profession or the school where they work.
- Keep their own mobile phones secure while in school – this is to avoid other people using them.
- Report any incidents of cyberbullying to the (Executive) Head Teacher.

There are no circumstances that will justify adults possessing indecent images of children.

Appendix 3 - 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://www.ico.org.uk/ Data Protection/Information Commissioner's Office (ICO)

Safe Schools and Communities team https://www.dorset.police.uk/police-forces/dorset-police/areas/about-us/local-support-and-guidance/ssct-young-people/ 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.

Appendix 4 – Relevant legislation

School staff should be aware of the legislative framework which currently surrounds use of social media / communication technology in the UK. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

Computer Misuse Act 1990

This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- "Eavesdrop" on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

Data Protection Act 1998

This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that personal data must be:

- Fairly and lawfully processed;
- Processed for limited purposes;
- Adequate, relevant and not excessive;
- Accurate;
- Not kept longer than necessary;
- Processed in accordance with the data subject's rights;
- Secure;
- Not transferred to other countries without adequate protection.

Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications Act 2003

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;

- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
- Ascertain whether the communication is business or personal;
- Protect or support help line staff.
- The school reserves the right to monitor its systems and communications in line with its rights under this act.

Trade Marks Act 1994

This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. youtube).

Telecommunications Act 1984

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice and Public Order Act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they: -

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Racial And Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Protection From Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Protection of Children Act 1978

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) and you arrange to meet them or travel to meet them (anywhere in the world) with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in any sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence. Children, Families and Education Directorate page 38 April 2007.

Obscene Publications Act 1959 and 1964

Publishing an “obscene” article is a criminal offence. Publishing includes electronic transmission.

Human Rights Act 1998

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of “higher law”, affecting all other laws. In the school context, human rights to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.