E-Safety Policy

Version:	v1.0
Policy Type:	People – Good Practice
Approval date:	28 January 2026
Approved by:	Trust Executive
Next review:	Autumn 2028

Together we Exceed

Contents

1. Introduction

1.1 The aim of this policy is to inform all staff of academy best practice around E Safety and draw attention to the related statements contained within existing Exceed Academies Trust Policy and national/local guidance on this subject. It is our responsibility to safeguard our pupils and protect our staff so that together we can ultimately maintain the safest possible e-learning and internet based working environments for everyone.

1.2 The term E Safety refers to both staff and pupil use of the internet, as well as mobile phones and other electronic based communication technologies including use of social media and social networks.

1.3 Whilst we appreciate the benefit of such online services, we also recognise that some adults will be suitably deviant enough to use these systems to abuse and harm our pupils and young people. It is important to reinforce that all staff have a duty of care to protect our pupils and young people from risk of harm and as such act in a way that does not call into question their suitability to work with children.

1.4 This policy has been created in line with national guidance issued by the Department for Education and CEOP (Child Exploitation & Online Protection Command) well as also drawing information from existing local guidance. It does not replace or take priority over other policy or guidance issued by Exceed Academies Trust and as such, this document should be read in conjunction with the associated policy and guidance documents listed below;

- Code of Conduct Policy
- Safer Working Practice Guidance
- ICT Acceptable Use Policy
- Data Protection Policy
- Data & E Security Breach Prevention Policy
- Data Breach Policy
- Disciplinary Policy & Procedure

1.5 Whilst care has been taken to consider all aspects of E Safety, there may be times when the Trust/Academy needs to make independent judgments on individual situations not covered in this document. It is expected that in these circumstances the Trust/Academy will seek advice from the People team.

1.6 This document applies to all members of staff employed either directly or indirectly by the Academy and the Trust and whether the place of work is permanent, temporary or peripatetic. All members of staff are expected to adhere to this policy to ensure the safety of the pupils they may come into contact with via their professional role. Any member of staff found to be in breach of these guidelines may be subject to disciplinary action.

1.7 For the purpose of this document ’pupils’ will refer to all children and young people, who members of staff have contact with as part of their professional capacity and to which all staff have a professional duty of care.

2. Scope

2.1 This policy applies to the following individuals in school;

- Staff
- Pupils
- Volunteers
- Any other users of school ICT systems

3. Roles and Responsibilities

Exceed Academies Trust Board of Trustees/CEO/Local Advisory Board

3.1 The Trust Board/CEO/Local Advisory Board has overall responsibility for monitoring this policy and holding the Headteachers to account for its implementation. The Trust Board/CEO/Local Advisory Board will co-ordinate regular meetings with appropriate staff to discuss online safety and monitor online safety records as provided by the Designated Safeguarding Lead (DSL).

3.2 Board members will:

- Ensure that they have read and understand this policy
- Agree and adhere to the Exceed Academies Trust Acceptable Use of ICT policy

Headteacher and Senior Leadership Team (SLT)

3.3 The Headteacher/SLT is responsible for ensuring;

- That all staff read and understand this policy
- For ensuring that the policy is being implemented consistently throughout the school
- The day-to-day implementation and management of this policy
- The overall allocation and provision of resources

This list is not exhaustive. It should be noted that the Headteacher/SLT would also be expected to adopt the responsibilities of all Trust staff, as shown below, in addition to the above.

Designated Safeguarding Lead(s)

3.4 Details of the academy designated safeguarding leads (DSL) and deputies are set out in the local school version of the Child Protection and Safeguarding Policy. The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the Headteacher/SLT to ensure that all school staff fully understand this policy and that it is being implemented consistently throughout the school
- Ensure staff attend relevant CPD, as and when required, to ensure their understanding of E Safety
- Working with the Headteacher/SLT, ICT Network Manager and other staff, as necessary, to address any online safety issues or incidents

- Ensuring that any online safety incidents are recorded 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 in relation to safeguarding and online safety
- Liaising with other agencies and/or external services if necessary

This list is not exhaustive. It should be noted that the DSL(s) would also be expected to adopt the responsibilities of all Trust staff, as shown below, in addition to the above.

ICT Management

3.5 The Trust ICT Lead 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 Trust ICT systems are secure and provide a high level of protection against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting security checks and monitoring all Trust/Academy ICT systems on a regular basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are recorded and managed appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are reported to the Headteacher immediately
- Assisting staff with authorised use of the ICT facilities and devices, as and when required
- Immediately reporting any breach of personal information or information leakage to the Data Protection Officer (DPO)
- Ensuring that all Trust and Academy owned devices are secured and encrypted in line with the Trust's Data Protection Policy

This list is not exhaustive. It should be noted that the Trust ICT Lead would also be expected to adopt the responsibilities of all Trust staff, as shown below, in addition to the above.

All Trust/Academy staff, volunteers, contractors and agency staff

3.6 All Trust and Academy staff, including contractors and agency staff, and volunteers/contractors are responsible for:

- Maintaining an understanding of this policy in conjunction with the Trust/Academy Safeguarding/Child Protection policies and the Safer Working Practice guidance
- Attending and completing all mandatory CPD, provided by the Trust/Academy
- Implementing this policy consistently
- Agreeing and adhering to the Exceed Academies Trust ICT Acceptable Use policy and ensuring that pupils adhere to the same
- Working with the Trust/Academy DSL(s) to ensure that any online safety incidents are recorded 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
- Understand the risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep pupils safe whilst they are online at school
- Recognising the additional risks that children with SEN and disabilities (SEND) face online, for example, from online bullying, grooming and radicalisation and are confident they have the ability to support SEND children to stay safe online.

This list is not intended to be exhaustive.

4. Social Contact with Pupils, Children or Young People

4.1 Staff must not establish or seek to establish social contact with pupils for the purpose of securing a friendship or to pursue or strengthen a relationship. Even if a pupil seeks to establish social contact, or if this occurs coincidentally, the member of staff should exercise his or her professional judgement in making a response and be aware that such social contact could be misconstrued. Members of staff should alert the Headteacher or Chief People Officer to any such contact immediately.

4.2 All contact with pupils should be through appropriate academy authorised channels at all times. Any communication outside of agreed professional boundaries could be prone to misinterpretation and as a result could put both the employee and pupils at risk.

4.3 Staff should not give, nor be required to give, their personal details such as home or mobile phone number, Instant Messenger or social media identities or personal e-mail address to pupils. Any member of staff found to be in contact with pupils through any of the above means, or any other unapproved method, without prior consent could be subject to disciplinary action.

4.4 Internal e-mail and approved contact systems should only be used in accordance with the Academy Code of Conduct and the Exceed Academies Trust ICT Acceptable Use Policy.

4.5 This means that members of staff should:

- always seek approval from senior management for any planned social contact with pupils for example when part of a reward scheme or pastoral care programme
- advise senior management of any regular social contact they have with a pupil, which may give rise to concern
- report and record any situation which they feel might compromise the reputation of the organisation or their own professional standing

5. Social Media – Business and Personal Use

5.1 Social media is a broad term for any kind of online platform, which enables people to directly interact with each other. It allows people to share information, ideas and views. Examples of social media include:

- Blogs
- Facebook

- LinkedIn
- X (formerly Twitter)
- WhatsApp
- Snapchat
- TikTok
- Google+
- Instagram
- Myspace
- Flickr
- YouTube

5.2 The Trust/Academy positively encourages the use of social media personally and within a professional environment, however, it is important that all staff ensure and maintain high levels of professionalism at all times whilst using social media. It is also important to create a distinction between the use of personal and professional social media accounts.

Business Use

5.3 Professional accounts linked to the Trust/Academy should be managed professionally by nominated staff, set up using academy e-mail addresses and follow the naming conventions guidelines. All posts must be suitable and appropriate, recognising that the internet is a public forum and once information is published online it is then in the public domain.

5.4 Certain circumstances will allow for contact with pupils via the Trust/Academy's professional social media accounts, however, all conversations and content must be appropriate and carried out by nominated staff. Attention should also be taken to posts or people 'followed' or 'liked' ensuring the related content is also suitable.

5.5 Secure and suitable strength passwords should be devised, and security settings should be applied so access to your personal profile and the information contained is limited to those explicitly given access.

5.6 Employees should seek permission from the Trust/Headteacher before creating an official Trust/Academy site explaining their business reasons for doing so.

5.7 Any official Trust/Academy sites created must not breach the terms and conditions of social media service providers, particularly regarding minimum age requirements.

5.8 Employees must, at all times, act in the best interests of pupils when creating, participating in or contributing content to social media sites.

5.9 If you are contacted for comments about the Trust/Academy for publication anywhere, including in any social media outlet please direct the enquiry to the Trust Chief Operating Officer or Governance Manager, along with the Headteacher.

5.10 With regard to personal safeguarding, you should report any harassment or abuse you receive online while using your work accounts.

Personal Use

5.11 It is recognised that personal access to Social Networking sites, outside the work environment, is at the discretion of the individual. However, members of staff should consider their use of social networks as they take on the responsibilities of a professional, taking particular care to secure personal information and ensure their use of such networking sites is respectable and appropriate at all times, including the published content of any personal pages. Accessing and direct usage of personal social media accounts during the working day is prohibited on any Trust/Academy or personal device and staff should be aware that failure to comply with this could result in disciplinary action.

5.12 Members of staff must not have any contact with pupils through personal social media accounts and staff must not add pupils as friends or respond to requests for friendship from children if asked; instead these requests should be declined. If a member of staff suspects that an existing friend is a pupil, child or young person, they should take reasonable steps to check the identity of that individual.

5.13 Employees must not have any contact with pupils' family members through personal social media if that contact is likely to constitute a conflict of interest or call into question their objectivity.

5.14 Information employees have access to as part of their employment, including personal information about pupils and their family members, colleagues, and other parties and Trust corporate information must not be discussed on their personal web space.

5.15 Trust/Academy email addresses and other official contact details must not be used for setting up personal social media accounts or to communicate through such media.

5.16 Personal profiles on social networking sites and other internet posting forums must not identify your employer or place of work and careful consideration should be given to information, which is published on such sites. For example, information which is confidential or could put others at risk should not be posted on such public domains. If the material you post or display is considered inappropriate or could be considered to bring your school or profession into disrepute, disciplinary action may be considered.

5.17 Caution is advised when inviting work colleagues to be 'friends' in personal social networking sites. Social networking sites blur the line between work and personal lives, and it may be difficult to maintain professional relationships.

5.18 Employees are advised that they set the privacy levels of their personal sites as strictly as they can and to opt out of public listings on social networking sites to protect their own privacy.

5.19 Employees should keep their passwords confidential, change them often and be careful about what is posted online. It is not appropriate to reveal home addresses, telephone numbers and other personal information.

5.20 Secure and suitable strength passwords should be devised and security settings should be applied so access to your personal profile and the information contained is limited to those explicitly given access.

5.21 For further guidance on social media networking and social contact with pupils please refer to academy Code of Conduct procedure and the Trust Safer Working Practice guidance document.

5.22 Any content or online activity, which raises a safeguarding concern must be reported to the DSL(s) in the Academy/Trust.

5.23 Any online concerns should be reported as soon as identified, as urgent steps may need to be taken to support the child.

6. Inappropriate Material

6.1 When considering what is defined as inappropriate material it is important to differentiate between inappropriate and illegal and inappropriate but legal. All staff should be aware that in the former, case investigation may lead to criminal investigation, prosecution, dismissal and barring. In the latter, it can still lead to disciplinary action, dismissal and barring even if there is no criminal prosecution.

Illegal Material

6.2 It is illegal to possess or distribute indecent images of a person under 18 and viewing such images on-line may constitute possession even if not saved. Accessing child pornography or indecent images of children on the internet, and making, storing or disseminating such material is illegal and if proven will invariably lead to the individual being barred from work with children and young people.

Material which incites hate, harm or harassment

6.3 There are a range of offences in relation to incitement of hatred on the basis of race, religion, sexual orientation and particular offences concerning harassing or threatening individuals which includes cyber bullying by mobile phone and social networking sites etc. It is an offence to send indecent, offensive or threatening messages with the purpose of causing the recipient distress or anxiety.

Professionally Inappropriate Material

6.4 Actions outside the workplace that could be considered so serious as to fundamentally breach the trust and confidence in the employee, may constitute Gross Misconduct. These actions may not always be illegal. For example, using work equipment to access inappropriate or indecent material, including 'adult pornography', will give the Trust or Academy rightful cause for concern, particularly if as a result children or young people might be exposed to inappropriate of indecent material. Such behaviour would be considered inappropriate and could result in disciplinary action.

6.5 Some examples of inappropriate material and actions are:

- Posting offensive or insulting comments about colleagues, parents, pupils or others on social networking sites;
- Accessing adult pornography on work-based computers during breaks;

- Making derogatory comments about colleagues, parents, pupils or others on social networking sites;
- Posting unprofessional comments about the teaching or education profession or workplace on social networking sites
- Making inappropriate statements or asking inappropriate questions about pupils on social networking sites
- Contacting pupils by email or social networking without senior staff approval
- Trading in fetish equipment or adult pornography.

7. Creating Images of pupils through Photography and Video

7.1 Many work-based activities involve recording images and these may be undertaken as part of the curriculum, extra school activities, for publicity, or to celebrate achievement. However, written permission should be gained from legal guardians as well as senior management prior to creating any images of pupils.

7.2 Using images of pupils for publicity purposes requires the age-appropriate consent of the individual concerned and their legal guardians. Images should not be displayed on websites, in publications or in a public place without such consent. The definition of a public place includes areas where visitors to the school or service provision have access.

7.3 Photograph or video images must be created using equipment provided by the workplace. It is not acceptable to record images of children on personal equipment such as personal cameras, mobile phones or video cameras without prior consent. Images of children must not be created or stored for personal use.

7.4 Members of staff creating or storing images of children using personal equipment without prior consent may be subject to disciplinary action.

7.5 Members of staff must:

- be clear about the purpose of the activity and about what will happen to the photographs when the lesson/activity is concluded
- ensure that senior management is aware that photography/image equipment is being used and for what purpose
- ensure that all images are available for scrutiny in order to screen for acceptability
- be able to justify images of children in their possession
- avoid making images in one-to-one situations

7.6 Members of staff must not take, display or distribute images of children unless they have consent to do so. Failure to follow any part of this code of practice could result in disciplinary action being taken.

7.7 For further guidance on creating, displaying and storing images of children please refer to the Academy/Trust Code of Conduct, Safer Working Practice guidance document as well as guidance from the Department for Education (Safeguarding Children in Digital Work) and CEOP (Child Exploitation and Online Protection unit)

8. Internet Use

8.1 Members of staff must follow and adhere to the policies on the use of ICT equipment at all times and must not share logins or password information with other members of staff, pupils, children or young people, friends, family or members of the public.

8.2 Members of staff should ensure that any internet-based content which they download is suitable and appropriately work based. Accessing sites which are not work related such as shopping and holiday websites as well as accessing personal social media accounts during work hours is not acceptable and could result in disciplinary action.

8.3 Under no circumstances should members of staff in the workplace access inappropriate images or web pages using either personal or work-based equipment. Accessing child pornography or indecent images of children on the internet, and making, storing or disseminating such material is illegal, and if proven, will invariably lead to disciplinary action and the individual being barred from work with children and young people.

8.4 Using work-based equipment to access inappropriate or indecent material, including adult pornography, either in the workplace or at home, whilst not necessarily illegal, will give cause for concern particularly if as a result children or young people might be exposed to inappropriate or indecent material and may also lead to disciplinary action.

8.5 For further information regarding safe internet use please refer to the Academy/Trust Code of Conduct procedure or ICT Acceptable Use policy

9. Use of personal technology/equipment in school

9.1 The use of any personal equipment in the academy should always be with the prior permission of senior management in order to comply with health and safety regulations, safer working practice guidance, data protection regulations. In doing so members of staff should take care to comply with all Trust and Academy ICT acceptable use policies and Codes of Conduct.

9.2 Personal equipment capable of recording images, moving images or sounds and those used for accessing the internet such as mobile phones, cameras, video cameras and laptops should not be used in work time without the prior permission of senior management.

9.3 Any member of staff found to be using such personal equipment without prior authorisation may be subject to disciplinary action.

10. Propriety and Behaviour

10.1 All members of staff have a responsibility to maintain public confidence in their ability to safeguard the welfare and best interests of pupils and young people. They should adopt high standards of personal conduct in order to maintain the confidence and respect of their peers, pupils, parents and the public in general.

10.2 Members of staff should not behave in a manner, which would lead any reasonable person to question their suitability to work with children or act as a role model. This includes behaviour in virtual online communities, as well day to day social situations. Members of staff also should not make (or encourage others to make) unprofessional personal comments through online media, which scapegoat demean or humiliate, or might be interpreted as such.

10.3 An individual's behaviour, either in or out of the workplace, should not compromise his or her position within the work setting nor bring the school or organisation into disrepute.

10.4 All staff should note that monitoring software is in active use on all academy electronic hardware and the content of all staff and student communications, including the use of Word, PowerPoint and Excel documents, is monitored for E Safety and security purposes at all times. Any member of staff highlighted as causing concern will be subject to investigation and may also be subject to disciplinary action.

10.5 If an allegation is received that a member of staff is responsible for comments made (online or otherwise) which could be deemed harmful, threatening, defamatory or abusive to the school or organisation, this will be investigated using the appropriate procedure. Any actions which bring the organisation or profession into disrepute will be considered under the appropriate policy and appropriate action taken in line with that procedure.

10.6 For further guidance on Propriety and Behaviour please refer to the Academy/Trust Code of Conduct and the Trust Safer Working Practice Guidance document

11. Confidentiality

11.1 Members of staff may have access to confidential information about pupils and the academy in order to undertake their everyday responsibilities and in some circumstances, this may be highly sensitive or private information. Such information should never be shared with anyone outside the Academy/Trust, a member of the public or outside agencies, except in specific circumstances, for example when abuse is alleged or suspected. In such cases, individuals have a duty to pass information on without delay, but only to those with designated child protection responsibilities or a senior member of staff.

11.2 Care should be taken with the storage of such confidential information. Confidential information should never be stored on personal computers or devices or distributed through personal e-mail or internet channels. Only authorised academy-based devices and systems should be used to store and transfer confidential information. Members of staff found to be compromising confidentiality by use of unauthorised systems and devices could be subject to disciplinary action.

11.3 The storing and processing of personal information in relation to pupils and others is governed by the Data Protection Act 2018 alongside UK GDPR. For further guidance in relation to confidentiality issues and safe storage of data please refer to the ICT Acceptable Use policy and the Data and Security Breach Prevention policy as well as the Academy/Trust Code of Conduct procedure and the Trust Safer Working Practice guidance document.

12. Cyberbullying

12.1 All forms of bullying, including cyberbullying, are taken very seriously. Bullying is never tolerated, and it is not acceptable for any member of staff to behave in a manner which is intimidating, threatening or in any way discriminatory. Behaviour which constitutes Bullying or Harassment may be dealt with under the Exceed Academies Trust Grievance or Disciplinary policies and could result in disciplinary action.

12.2 However, this does not just extend to behaviour within the workplace. In some instances, bullying or harassment that occurs outside the workplace where there is a link to employment could also fall under the responsibility of the employer and therefore result in disciplinary action being taken against the responsible individual.

12.3 Certain activities relating to cyberbullying could be considered criminal offences under a range of different laws. Cyberbullying consists of threats, harassment, embarrassment, humiliation, defamation or impersonation and could take the form of general insults, prejudice-based bullying or discrimination through a variety of media. Media used could include e-mail, Virtual Learning Environments, chat rooms, web sites, social networking sites, mobile and fixed-point phones, digital cameras, games and virtual world sites.

12.4 It is recognised that members of staff, as well as pupils, may become targets of cyberbullying. Members of staff should never engage with or retaliate to incidents of cyberbullying and should report any such incidents appropriately. Staff should report any work-based incidents to their line manager immediately who should provide support and facilitate any investigation required. Members of staff who wish to seek additional support or advice would be advised to contact their union representative or professional association.

12.5 If an allegation is received that a member of staff is responsible for comments made online which could be deemed harmful, threatening, defamatory, abusive or harassing in any way towards another employee, the academy will investigate this matter. Any allegation of bullying or harassment made by an employee against another member of staff where the accused uses the internet, mobile phone, text message or e-mail, along with any other forms of abuse, will be dealt with through the Trust Grievance Procedure and could lead to disciplinary action.

12.6 Staff are required to take steps to protect themselves and their personal information by:

- Keeping all passwords secret and protect access to their online accounts
- Not befriending children and young people via personal social networking services and sites
- Keeping personal phone numbers private
- Not using personal phones to contact parents and pupils, children and young people
- Keeping personal phones secure, i.e. through use of a pin code, when within work
- Not posting information about themselves that they would not want employers, colleagues, pupils, children, young people or parents to see
- Not retaliating to any incident
- Keeping evidence of any incident
- Promptly reporting any incident using existing routes for reporting concerns.