

ENDEAVOUR HIGH SCHOOL

E-SAFETY Policy



Headteacher: Mr S Edgell

E Safety Guidance for Endeavour High School

1. Introduction

1.1 The aim of this guidance is to inform all staff of best practice around E Safety and draw attention to existing local and national guidance on this subject. It is our responsibility to safeguard young people and protect staff from false accusations of improper conduct so that together we can ultimately maintain the safest possible learning and working environments for children and staff alike.

1.2 This document has been created in line with national guidance issued by the Department for Children, Schools and Families as well as also drawing information from existing policies issued by Endeavour High School. It does not replace or take priority over other advice or codes of conduct issued by Endeavour High School or any National Guidance issued by other sources. As such this document should be read in conjunction with the associated guidance documents listed below.

- Internet Access Policy (Apr 2009)
- ICT Security Policy (Apr 2009)

1.3 Whilst care has been taken to consider all aspects of E Safety there may be times when members of staff need to make independent judgments on individual situations not covered in this document. It is expected that in these circumstances that all staff will advise their senior colleagues of such action taken or proposed and the school will seek further advice from HR.

1.4 This document applies to all members of staff employed either directly or indirectly by Endeavour High School. All members of staff are expected to adhere to this code of practice to ensure the safety of the young people in their care and in doing so fully abide by the guidance contained herein. Any member of staff found to be in breach of these guidelines may be subject to disciplinary action.

1.5 For the purpose of this document 'Students', 'Pupils', 'Children' and 'Young People' 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. Social Contact with Pupils, Children or Young People

2.1 Staff must not establish or seek to establish social contact with pupils, children or young people for the purpose of securing a friendship or to pursue or strengthen a relationship. Even if a pupil, child or young person 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.

2.2 All contact with pupils, children or young people should be through appropriate 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 young person at risk.

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

2.4 This means that members of staff should:

- always seek approval from senior management for any planned social contact with pupils, children or young people for example when it is part of a reward scheme or pastoral care programme
- advise senior management of any regular social contact they have with a pupil, child or young person 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

Social Networking Websites

2.5 This also extends to use of Social Networking sites. Members of staff must not have any contact with pupils, children or young people through such sites and staff must not add pupils, children or young people as friends or respond to requests for friendship from children if asked. If a member of staff suspects that an existing friend is a student, child or young person, they should take reasonable steps to check the identity of the individual and end the friendship should the suspicions not be put to rest

2.6 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.

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

2.8 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 the school or profession into disrepute, disciplinary action may be considered.

3. Inappropriate Material

3.1 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

3.2 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

3.3 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

3.4 Actions outside the work place 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 school or service rightful cause for concern particularly if as a result children or young people might be exposed to inappropriate or indecent material. Such behaviour would be considered inappropriate and could result in disciplinary action.

3.5 Some examples of inappropriate material and actions are:

- Posting offensive or insulting comments about colleagues on social networking sites;
- Accessing adult pornography on work based computers during break;
- Making derogatory comments about pupils or colleagues on social networking sites;
- Posting unprofessional comments about ones 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.

4. Creating Images of pupils through Photography and Video

4.1 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 children.

4.2 Using images of children 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.

4.3 Photograph or video images must be created using equipment provided by the work place. 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.

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

4.5 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

4.6 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.

5. Internet Use

5.1 Members of staff must follow and adhere to the policies on the use of IT 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.

5.2 Under no circumstances should members of staff in the work place access inappropriate images 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 the individual being barred from work with children and young people.

5.3 Using work based equipment to access inappropriate or indecent material, including adult pornography, either in the work place or at home, 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.

6. Use of personal technology/equipment in school

6.1 The use of any personal equipment in schools should always be with the prior permission of senior management in order to comply with health and safety regulations and members of staff should take care to comply with acceptable use and IT policies.

6.2 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.

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

7. Propriety and Behaviour

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

7.2 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.

7.3 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.

7.4 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.

8. Confidentiality

8.1 Members of staff may have access to confidential information about pupils, children or young people and the school in order to undertake their every day responsibilities and in some circumstances this may be highly sensitive or private information. Such information should never be shared with anyone outside the school, 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.

8.2 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 email or internet channels. Only authorised school 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.

8.3 The storing and processing of personal information about pupils is governed by the Data Protection Act 1998.

9. Cyberbullying

9.1 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 Bullying and Harassment Policy and could result in disciplinary action.

9.2 However, this doesn't just extend to behaviour within the work place. 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.

9.3 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 email, Virtual Learning Environments, chat rooms, web sites, social networking sites, mobile and fixed-point phones, digital cameras, games and virtual world sites.

9.4 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 school 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 email, along with any other forms of abuse, may be dealt with through the Bullying and Harassment policy and could lead to disciplinary action.

9.5 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 on 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 wouldn't 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.

9.6 Any incident of cyberbullying will be investigated under the appropriate policy and could result in disciplinary action.