E-Safety Policy

(Incorporating Acceptable Use)

The Eastwood Academy

Believe, Succeed, Together

Author's Name:	Mr. N. Houchen
Date Reviewed	June 2016
Date Ratified by Governing Body	
Signature of Principal	
Signature of Chair of Governors	

Contents

1.0 E-Safety

ICT in the 21st Century has an all-encompassing role within the lives of children and adults. Current and emerging technologies (see below) have a range of educational and social benefits, but their usage requires transparent delineation in order to educate, support and protect all parties i.e. pupils, staff and the Academy.

- Internet.
- E-mail.
- Instant messaging often using simple web cams.
- Blogs.
- Podcasting.
- Social networking sites.
- Video broadcasting sites.
- Chat Rooms.
- Gaming Sites.
- Music download sites.
- Mobile phones with camera and video functionality.
- Smart phones with e-mail, web functionality and Office applications.

Ofsted describes 'e-safety' as a *'school's ability to protect and educate pupils and staff in their use of technology as well as having appropriate mechanisms in place to intervene and support any incident where appropriate'.*

1.1 Training

Vice Principal, Mr. C. Niner, has undertaken accredited EPICT training and is a CEOP Ambassador.

As part of the Induction Programme, all staff receive the equivalent of Level 1 Certificate in E-Safety Awareness.

1.2 Education and Awareness

1.21 Parents

The Academy holds an annual 'E-Safety Evening' in October which Year 7 parents are invited to attend. The evening involves a presentation from Senior Leaders and an 'e-clinic' where parents can ask specific questions.

Following the evening, parents are offered access to an online Level 1 e-safety awareness course, should they wish to avail this opportunity.

The Academy's website has an e-safety section specifically for parents with information on how to keep their child safe online, a parents' guide to the internet and a range of resources such as those relating to setting up safety features and parental controls.

1.22 Pupils

Year 7 and Year 8 pupils complete an e-safety module as part of the Computing curriculum. In addition, 'keeping safe online' is included in the PSHE curriculum.

In addition to e-safety education delivered through PSHE, Year 9 pupils have an opportunity to complete a BCS Level 1 accredited e-safety qualification.

Year 10 and 11 pupils receive e-safety education through PSHE.

E-safety awareness, delivered by the CEOP Ambassador, form part of the annual assemblies programme for all year groups.

The Academy's website has an e-safety section specifically for pupils with information and a link to the main risks or problems associated with the internet and mobile technology and the contact details of support services (including reporting abuse through CEOP).

2.0 ICT Acceptable Use – Academy Staff

All staff using ICT equipment within the Academy must ensure that they have read and abide by the Acceptable Use Policy. If they are found to have contravened any of the requirements they may face disciplinary action under the Disciplinary Misconduct Policy.

The Academy's ICT systems and network cannot be regarded as private, and user accounts will be subject to random monitoring. They should be used primarily for school purposes, conform to the norms of moral decency and not contravene ICT or other relevant legislation e.g.

- Data Protection Act 1998.
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Human Rights Act 1998.

2.1 General Use of ICT

When using ICT equipment staff should not:

- Give anyone access to their username or password (unless authorised by the Principal).
- Attempt to introduce any unlicensed applications.
- Corrupt, interfere with or destroy any other user's information.
- Release any personal details of any colleague or pupil.
- Use the Academy internet access for business, profit, advertising or political purposes.
- Knowingly misuse or mistreat ICT equipment. Staff are encouraged to take their tablet pc off the premises for home use, but this should be principally for school-related activities.
- Leave their account open at the end of a session.
- Engage in any activity which might compromise the security of the Academy network.

2.2 Use of E-mail

When using e-mail staff should:

- Observe 'netiquette' on all occasions. E-mail should not be considered a private medium of communication and great care should always be taken over content, because of the possibility of public scrutiny.
- Not include offensive or abusive language in my messages or any language which could be considered defamatory, obscene, menacing or illegal.
- Not use language that could be calculated to incite hatred against any ethnic, religious or other minority.
- Make sure that nothing in messages could be interpreted as libellous.
- Not knowingly send any message which is likely to cause annoyance, inconvenience or needless anxiety.

2.3 Use of the Internet

When using the internet staff should:

- Under no circumstances view, upload or download and material which is likely to be unsuitable for children. This applies to any material of a violent, dangerous or inappropriate sexual content.
- Check copyright before publishing any work and ensure that any necessary permission is obtained.
- Refrain from using social networking sites or instant messaging services, particularly where personal information is placed in the public domain and their professional status and position could possibly be compromised.

2.4 Abuse of E-mail/Internet

The Academy will not accept any abuse of telecommunication technology e.g. e-mail/internet or telephones. Such behaviour may result in disciplinary action in accordance with the Disciplinary Misconduct Policy.

The downloading, sending or accessing of offensive material that affect the dignity of any individual or group of individuals at work may constitute harassment under the **Protection from Harassment Act 1997** and **Telecommunications Act 1984.** Threatening, obscene or harassing messages including chain e-mails and material that will cause offence and/or degrade individuals or minority groups will constitute a disciplinary offence which may result in dismissal.

Under the **Obscene Publications Act 1959** an employee may have criminal liability if an individual publishes material that could corrupt or deprave the persons likely to see the material, this includes the transmission of data stored electronically.

Staff are also reminded of inappropriate behaviour involving the use of the internet, including conversing with pupils via e-mail and/or social networking sites. Such behaviour may result in disciplinary proceedings, including dismissal.

2.5 Use of Cameras and Digital Photographic Technology

This is detailed explicitly in the following DfE guidance.

http://www.southend.gov.uk/resources/Safeuseofimages.pdf

A précis of the pertinent points of this guidance are as follows:

- Parental permission must be sought in advance of any photos and/or digital recordings being taken of pupils.
- Where children are in Public Care (Looked After) staff must gain consent on the corporate parent's behalf from the social worker.
- If you use a photograph, avoid naming the pupil in full (first name and surname).
- If a pupil is named in full in the text of a publication, avoid using their photograph.
- You should also check that you have not inadvertently named a child in a photo because they are wearing a name badge. Children can be identified by logos or emblems on sweatshirts. Remove these before the photograph is taken, or blank them out in the production process.

Staff are also reminded that under The Children Act 2004 it is illegal to take indecent photos of children or to create indecent pseudo images of children (under 18's). Such matters are likely to be pursued by other agencies e.g. Police and Social Services, but will also be dealt with under the Disciplinary Misconduct Policy.

2.6 Staff Use of Mobile Phones

Staff are not discouraged from bringing a mobile phone onto the premises, but should be avoid flagrant public use that conflicts or compromises their professional status and/or maintaining good order and discipline.

3.0 ICT Acceptable Use – Pupils

The policy is conveyed to parents and pupils principally in the Pupil Planner (see below) but also through assemblies and at relevant points in the curriculum.

In relation to the Academy computer network, and associated school-based ICT resources, I agree to adhere to the following:

- Only use the computer network for school-related work.
- Only log on using my own username and password.
- Regularly change my password and never disclose it to other pupils.
- Refrain from knowingly accessing (or attempting to access) any links that could be considered inappropriate or offensive because of pornographic, racist, homophobic, violent or illegal content.
- Never seek to harass or abuse fellow pupils and/or members of staff, either on the school network or via e-mail, instant messaging services or external social networking sites, and will report any cases of such usage against me.
- Report to a member of staff or a parent any communication online or any material that makes me uncomfortable or asks me for personal information that I do not want to provide.

- Never reveal personal information including names, addresses, telephone numbers and photographs of myself or others.
- Respect the copyright nature of material that I may find on the internet.
- Never use downloaded material unless it is properly sourced and referenced.
- Never intentionally waste resources e.g. paper.
- Report any accidental damage immediately to a member of staff.
- Never interfere with or damage the school computer network in any way.
- Report any misuse of the school computer network to a member of staff.

I understand that my school account is not, and cannot be, regarded as private and will be subject to random monitoring. I understand that if I am found not to be complying with this policy, I will be denied access to the computer network for a time determined by the Vice Principal. I also understand that I may face further disciplinary action depending on the nature of the offence.

3.1 Pupil Use of Mobile Phones and Unnecessary Electronic Equipment

This is detailed in the Behaviour and Discipline Policy.

4.0 Filtering and Monitoring

Filtering (at source) is provided by the service provider (Local Authority). In addition, the Academy has filtering software in place called Forefront TMG provided by Microsoft. The Academy uses TMG to create rules which are used to only allow access to the internal network form the outside world.

There are contrasting rulesets for pupils and staff to allow for a more flexible approach and age differentiation.

A report is produced on a weekly basis and random checks are made regarding the nature of the sites accessed by staff and pupils.

Sites are blocked when either monitoring and/or detection indicate their inappropriateness.

If issues arise with pupils, these are addressed under the Behaviour and Discipline Policy.

If issues arise with staff, these are addressed under the Disciplinary Misconduct Policy.