Montgomery High School

E-Safety Policy

Scope

This policy applies to all members of the Academy community (including staff, students / pupils, volunteers, parents, carers, visitors, community users) who have access to and are users of academy ICT systems, both in and out of the Academy.

The Education and Inspections Act 2006 empowers Principals to such extent as is reasonable, to regulate the behaviour of students when they are off the academy site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of the academy, but is linked to membership of the academy. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The academy will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents or carers of incidents of inappropriate e-safety behaviour that take place out of school.

Internet Safety

The internet can offer educational and social benefits to students and adults with technologies such as mobile phones, tablets, computers and games consoles. However, it is also important to consider the risks associated with these technologies, students could unknowingly expose themselves to danger, and adults could be a target for identity theft. Comments posted on social networking sites have led to students being bullied and staff being disciplined.

Risks associated with the internet, mobiles and social networking sites include:

- Cyberbullying
- Grooming
- Potential abuse by online predators
- Identity theft
- Exposure to inappropriate content
- Racist
- Hate
- Pornography

Roles and Responsibilities

The school will take all reasonable precautions to ensure e-Safety. However, owing to the scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. The Academy cannot accept liability for material accessed, or any consequences of, internet access.

E-Safety Coordinator will:

The e-safety Coordinator for Montgomery High School is Gill Smith.

- leads the e-safety committee
- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provides training and advice for staff
- liaises with the Academy Board and FCAT Safeguarding Board
- liaises with school technical staff
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments, meets regularly with e-Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- attends relevant meetings
- reports regularly to Senior Leadership Team

The Academy Council (or e-safety Governor) will:

- regular meetings with the e-safety Co-ordinator
- regular monitoring of e-safety incident logs
- regular monitoring of filtering / change control logs
- reporting to Academy Board and FCAT Safeguarding Board

Academy will:

- Provide a safe environment for students and staff.
- Block/ filter access to social networking sites and other inappropriate websites.
- Advise students never to give out personal details of any kind that may identify them or their location.
- Monitor internet usage and report any inappropriate use to child welfare officer.

Staff will:

- Staff accept that the Academy can monitor internet usage to help ensure staff and student safety.
- Confiscate items such as mobile phones, iPods, tablets etc. when they are being used to cause a disturbance in class or otherwise contravene the school behaviour/anti-bullying policy.
- Report anything inappropriate they find on the internet.
- Websites used will be viewed by staff prior to any lessons.
- Staff should not be accessing the internet for personal reasons while teaching students.

Students will:

- Only use approved e-mail accounts on the school network.
- Must immediately tell a teacher if they see any inappropriate material.
- Must not reveal personal details of themselves or others.
- Must not intentionally view inappropriate material on any device.

Education

Students

E-safety at Montgomery High School is focused in all areas of the curriculum and staff reinforce e-safety messages across the curriculum.

- A planned e-safety curriculum is provided as part of Computing, PHSE and other lessons and is regularly revisited.
- Key e-safety messages are reinforced as part of a planned programme of assemblies and pastoral activities
- Students are taught in lessons to be critically aware of the materials or content they access on-line and are guided to validate the accuracy of information.
- Students are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students are helped to understand the need for the student Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff act as good role models in their use of digital technologies, the internet and mobile devices
- In lessons where internet use is pre-planned, students are guided to sites checked as suitable for their use and we have processes in place for dealing with any unsuitable material that is found in internet searches.
- Where students are allowed to freely search the internet, staff are vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff temporarily remove those sites from the filtered list for the period of study. Any request to do so, will be auditable, with clear reasons for the need.

Staff

- A planned programme of formal e-safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the e-safety training needs of all staff will be carried out regularly. It is expected that some staff will identify e-safety as a training need within the performance management process.
- All new staff will receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Agreements.
- The E-Safety Coordinator will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- The E-Safety policy and its updates will be presented to and discussed by staff in staff meetings and INSET days.
- The E-Safety Coordinator will provide advice and training to individuals as required.

Governors

- Attendance at training provided by the Local Authority / National Governors Association / or other relevant organisation.
- Participation in school training / information sessions for staff or parents

Parents and Carers

The school will seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, e safety updates and web site
- Parents and carers evenings
- Reference to the relevant web sites / publications

Sanctions

Whenever a student or staff member infringes the e-Safety Policy, the final decision on the level of sanction will be at the discretion of the school management.
The following are provided as examples:

Students
Level 1 infringement

- Use of non-educational sites during lessons
- Unauthorised use of email
- Unauthorised use of mobile phone (or other new technologies) in lessons e.g. to send texts to friends
- Use of unauthorised instant messaging / social networking sites

[Possible Sanctions: referred to Faculty Director, e safety Coordinator, confiscation of phone]

Level 2 infringements

- Continued use of non-educational sites during lessons after being warned
- Continued unauthorised use of email after being warned
- Continued unauthorised use of mobile phone (or other new technologies) after being warned
- Continued use of unauthorised instant messaging / social networking sites
- Use of File sharing software
- Accidentally corrupting or destroying others' data without notifying a member of staff of it
- Accidentally accessing offensive material and not notifying a member of staff of it

[Possible Sanctions: referred to Faculty Director, e safety Coordinator, removal of Internet access rights for a period, confiscation of phone and contact with parent]

Level 3 infringements

- Deliberately corrupting or destroying someone's data, violating privacy of others
- Sending an email or message that is regarded as harassment or of a bullying nature (one-off)
- Deliberately trying to access offensive or pornographic material

[Possible Sanctions: referred to Faculty Director, e safety Coordinator, Principal, removal of Internet rights for a period and contact with parents]

Level 4 infringements

- Continued sending of emails or messages regarded as harassment or of a bullying nature after being warned
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988
- Bringing the school name into disrepute

[Possible Sanctions – Referred to Principal, Contact with parents, possible exclusion, refer to PCSO and e-safety officer]

Other safeguarding actions:

1. Secure and preserve any evidence

2. Inform the sender's e-mail service provider if a system other than the school system is used.

Pupils are also informed that sanctions can be applied to e-safety incidents that take place out of school if they are related to school.

Staff
Level 1 infringement (Misconduct)

- Excessive use of Internet for personal activities not related to professional development e.g. online shopping, personal email, instant messaging etc.
- Misuse of first level data security, e.g. wrongful use of passwords
- Breaching copyright or license e.g. installing unlicensed software on network

[Sanction – Principal. Warning given]

Level 2 infringement (Gross Misconduct)

- Serious misuse of, or deliberate damage to, any school / Council computer hardware or software;
- Any deliberate attempt to breach data protection or computer security rules;
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent;
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988;
- Bringing the school name into disrepute.

[Sanction – Referred to Principal/Academy Council and follow school disciplinary procedures; report to Human resources, report to Police.]

Other safeguarding actions:

1. Remove the PC to a secure place to ensure that there is no further access to the PC or laptop.
2. Instigate an audit of all ICT equipment by an outside agency, such as the schools ICT service providers - to ensure there is no risk of pupils accessing inappropriate materials in the school.
3. Identify the precise details of the material.

Rewards

Whilst recognising the need for sanctions it is important to balance these with rewards for positive reinforcement. The rewards can take a variety of forms – eg. Ambition Points for good research skills, certificates for being good cyber citizens etc.

Monitoring and reporting

a). The impact of the e-safety policy and practice is monitored through the audit of e-safety incident logs, behaviour logs, surveys of staff, students, parents and carers

b). The records are audited and reported to:

- the academy's senior leaders
- The academy council

- FCAT safeguarding board
- Blackpool Safeguarding Children Board (BSCB)

c). The academy action plan indicates any planned action based on the above.

For further help and support you can access the following pages:

- http://ceop.police.uk/safety-centre/11-16/
- http://www.bullying.co.uk/cyberbullying/
- http://www.childline.org.uk/Explore/Bullying/Pages/online-bullying.aspx