E-Safety Policy

Created: September 2018
Principal Author: James Heaver
Approved: October 2019
Approved by: Finance and Resources Committee
Date to be reviewed: October 2021

1. **eSafety - Roles and Responsibilities**
   1.1 As eSafety is an important aspect of strategic leadership within the school, the Principals and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. All e-safety coordination comes through the Safeguarding Team at the Academy with ultimate responsibility being with the Designated Safeguarding Lead (DSL). All members of the Academy community have been made aware of who to speak with in regards to E-Safety. It is the role of the DSL and safeguarding team to keep abreast of current issues and guidance through organisations such as CEOP (Child Exploitation and Online Protection) and Childnet.
   1.2 The Senior Leadership Team and Governors are updated by the DSL and safeguarding team and all governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.
   1.3 This policy, supported by the school's ICT Acceptable Usage Agreements for staff, governors and students (Appendix 1), is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: child protection, health and safety, behaviour and anti-bullying.

2. **eSafety in the Curriculum**
   2.1 ICT and online resources are increasingly used across the curriculum and can help to raise educational standards and promote pupil achievement. We believe it is essential for eSafety guidance to be given to students on a regular and meaningful basis. eSafety is embedded within the curriculum and we continually look for new opportunities to promote eSafety.
   2.2 Educating students on the dangers of technologies that may be encountered outside school is done informally and as part of the eSafety curriculum, e.g. Anti- Bullying Week, assemblies and specific eSafety training with selected year groups.
   2.3 Students are taught about relevant eSafety topics such as respecting other people's information and images, through discussion and class activities. Students also take part in topic specific PSHE days where eSafety is covered and this is also supported in residential care PSHE themed evenings.
   2.4 Students are made aware of the impact of Cyber-bullying and how to seek help and block unwanted contact if they are affected by any form of online bullying. Students are also aware of where to seek advice or help if they experience problems when using the internet and related technologies;

i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Childline.

3. eSafety Skills Development for Staff

3.1 Staff receives information and training on eSafety issues from memos and circulars, staff meetings and inset / courses. New staff given copies of the 'ICT Acceptable Usage Agreement and Code of Conduct at induction', which gives an overview of the eSafety issues, and key expectations for the Academy. All staff are expected to sign a copy of the ICT Acceptable Usage Agreement, which is retained in their HR file. .

3.2 All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of eSafety and know what to do in the event of misuse of technology by any member of the school community.

3.3 All staff are encouraged to incorporate eSafety activities and awareness within their curriculum areas wherever possible and relevant.

4. Managing the School eSafety Messages

4.1 We endeavour to embed eSafety messages across the curriculum whenever the internet and/or related technologies are used.

4.2 eSafety posters will be prominently displayed.

5. Incident Reporting

5.1 Any safeguarding concerns, unauthorised use or suspected misuse must be reported to the DSL and safeguarding team as per our Safeguarding Policy.

5.2 Incidents of Cyber bullying will be addressed through the school's anti bullying procedures.

5.3 Any security breaches or attempts, virus notifications, unsolicited emails or loss of equipment must be reported to the DSL, IT Manager and Data Protection Officer (DPO).

6. Misuse and Infringements

6.1 Complaints

6.1.1 Complaints and/or issues relating to eSafety should be made using the Academy's complaints policy.

6.2 Inappropriate Material

6.2.1 All users are aware that accidental access to inappropriate material must be immediately reported to the DSL and safeguarding team.

6.2.2 Deliberate access to inappropriate materials by any user will lead to the incident being logged by the DSL. Depending on the seriousness of the offence our disciplinary policy for staff or behaviour policy for students may be used. The following steps may be taken; investigation by Co-Principals or nominated individual, immediate suspension/exclusion, possibly leading to dismissal/permanent exclusion and involvement of police for very serious offences.

6.2.3 Users are made aware of sanctions relating to the misuse or misconduct through training and our policies found on Sharepoint.

6.3 Restriction of access

6.3.1 Any safeguarding concerns, unauthorised use or suspected misuse may result in the restriction of students accessing electronic devices. This may include; restriction

or confiscation of electronic devices, access restrictions to the academy WIFI or device apps, implementation of supervision when using electronic devices.

Appendix 1

Staff and Volunteer ICT Acceptable Usage Agreement

This agreement must be read in conjunction with the Social Media Policy, Academy Code of Conduct, Data Protection policy and E-safety policy, which are distributed at staff induction and are available under the HR policies section of Sharepoint.

1. I understand that the Academy will monitor my use of the ICT systems, email and other digital communications.

2. I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password and should log off the network when leaving work stations unattended.

3. I will immediately report any illegal, inappropriate or harmful material or incident to the Safeguarding team, IT manager and the HR manager.

4. I will not access, copy, remove or otherwise alter any other user's files, without their express permission.

5. I will communicate with others in a professional manner, I will not use aggressive, bullying or inappropriate language and I appreciate that others may have different opinions.

6. I will ensure that if I take images of others I will do so with their permission and in accordance with the Academy's policies. I will not use my personal equipment to record these images. Where these images are published (e.g. On the Academy website) it will not be possible to identify by name, or other personal information, any who are featured.

7. I will not use electronic chat or social networking sites to communicate with students, parents or carers. Communication on the official academy social media platforms is permitted provided it is in line with the Social Media policy.

8. I will only communicate with students (current or former) and parents or carers (current or former) using official Academy systems. Any such communication will be professional in tone and manner. The use of personal email and personal mobile phones is not permitted.

9. I will not engage in any on-line activity that may compromise my professional responsibilities or bring the Academy into disrupute.

10. I will not use personal email addresses for Academy related business.

11. I will respect the technical safeguards which are in place. Any attempt to breach technical safeguards, conceal network identities, or gain unauthorised access to systems and services is unacceptable.

- *I understand that the Academy reserves the right to monitor my emails and internet usage, but will endeavour to inform me if such monitoring takes place on my own account. I am aware that the Academy considers the following to be valid reasons for checking an employee's email:*

o *If the employee is absent for any reason and communications must be checked for the smooth running of the business to continue.*
o *If the Academy suspects that the employee has been viewing or sending offensive or illegal material, such as material containing offensive terminology or nudity (although the Academy understands that it is possible for employees inadvertently to receive such material and they will have the opportunity to explain if this is the case).*
o *If the Academy suspects that an employee has been using the email system to send and receive an excessive number of personal communications.*
o *If the Academy suspects that the employee is sending or receiving emails that are detrimental to the Academy.*
o If the Academy suspects that an employees has been excessively using the internet system for personal reasons

Internet access:

- *I understand that the Academy reserves the right to deny email and internet access to any employee at work, although in such a case it will endeavour to give reasons for doing so.*

I understand that if I fail to follow the principles set out in this agreement then formal action may be taken against me as per the Academy's Disciplinary policy.

I have read and understand the above and agree to use the Academy ICT systems (both in and out of Academy) and my own devices (in Academy and when carrying out communications related to the Academy) within the eSafety and Social Media Policies.

Staff/Volunteer Name	
Signed	

Date

If you are unclear about any of the points in the Acceptable Usage Agreement

please contact: Human Resources.

Appendix 2

Student ICT Acceptable Usage Agreement

1. I understand that the Academy will monitor my use of the ICT systems, email and other digital communications.

2. I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password and should log off the network when leaving computers unattended.

3. I will immediately report any illegal, inappropriate or harmful material or incident to a member of staff.

4. I will use electronic devices appropriately and not access any illegal, inappropriate or harmful material.

5. I will not access, copy, remove or otherwise alter any other student's files.

7. *I will ensure that if I take images of others I will do so with their permission.*

8. *When taking photographs, videos, video messaging or live streaming I will respect the privacy of those around me. Unless I have someone's direct consent, I will ensure they are not visible or audible.*

9. *I will not use chat or social networking sites to bully, intimidate or harass.*

10. *I understand that in the event of a safeguarding concern, unauthorised use or suspected misuse I may have my electronic device usage restricted.*

I have read, understand and agree to the above:

Student Name:

Signed:

Date: