COMDA-06-E-SAFETY

1 INTRODUCTION

1.1 E-safety encompasses internet technologies and electronic communications, the benefits, and risks of using them and provides safeguards and awareness for users, inside and outside of the Trust, to enable them to control their online experiences.

1.2 It is vital that the users of the Trust's computer systems are protected from potential harm that may be considered an E-safety issue.

1.3 All staff and students of the Trust are responsible for E-safety.

2 ROLE OF TRUST BOARD AND COMMITTEES

2.1 The Trust Board has overall responsibility for ensuring compliance with all relevant safeguarding, data protection and copyright obligations.

3 ROLE OF PRINCIPAL AND SENIOR LEADERSHIP TEAM

3.1 The Principal, the Communications Manager and the Network Manager are responsible that this policy is followed by all users of the Trust's equipment/Internet Service Provision.

3.2 The Principal delegates the responsibility for e-safety education and monitoring to the person appointed to that role.

4 SAFE AND RESPONSIBLE USE OF THE TRUST'S EQUIPMENT/INTERNET SERVICE PROVISION

4.1 The Trust promotes the safe use of internet-based websites and applications following current advice:

- Via the school website,
- Via education/assemblies – co-ordinated by the person appointed to the role.

4.2 All use of the Trust's equipment is monitored and traceable to the logged in user.

4.3 As far as is practicable, Wi-Fi access to the Trust's network, on private devices, is monitored.

4.4 Public facing documentation is controlled via the Communications Manager.

4.5 Access to internet material is controlled via Network Manager, who is able to block unsuitable sites and those not related to the educational purposes of the Trust.

5 USE OF THE INTERNET AND INTERNET BASED RESOURCES

5.1 Internet access is available to all students and staff. Access must be removed after extreme or repeated contravention of the Acceptable User Policy.

5.2 All users must comply with copyright laws.

6 THE TRUST WEBSITE

6.1 Only essential contact details must be presented:

6.1.1 Personal information must be excluded, this includes, but is not limited to:

- Photographs, if appropriate consent has not been obtained,
- Full Names.

6.1.2 Information which would enable email harvesting will be minimised.
Email harvesting is the collection of email addresses for the purposes of spamming. The methods of collecting this information include purchasing it, stealing it, or phishing (where a person responds to an unsolicited email).

6.2 Copyrights and property rights will be respected for:

- Student work,
- Work produced outside the Trust.

7 E-SAFETY ISSUES WHICH ARISE ON PERSONAL DEVICES

7.1 These are outside the remit of the Trust.

7.2 The Trust will be sensitive to external experiences and will co-operate with external legal bodies as required:

7.2.1 Where appropriate, parent/carers must be informed.

8 SECURITY AND FILTERING

8.1 The IT system of the Trust will be regularly reviewed; the Network Manager is responsible for ensuring that this happens.

8.2 Up to date anti-virus software will be installed and updated regularly. It is used to scan files and programs on the system to ensure the system remains “clean” of malware.

8.3 Unapproved system utilities and executable files are specifically forbidden from student user areas and emails, with the exception of:

- Students with Computer Science examinations when the Curriculum Leader for Computer Science has requested it,
- Following specific guidelines and arrangements as agreed with the Network Manager.

8.4 E-safety is managed by filtering software:

- The Network Manager ensures that filtering and monitoring systems are as effective as possible given the ever-changing online environment:
  - Barracuda email protection – is used by the Trust to reduce e-safety threats via email,
  - Smoothwall Education and Wellbeing Monitoring – is used by the Trust to detect online risks.
- Staff and students must report unsuitable sites to the Network Manager,
- Safeguarding protocols must be followed, if appropriate,
- If illegal material is discovered it must be reported to the criminal agencies e.g., police, Child Exploitation and Online Protection (CEOP).

9 EMERGING TECHNOLOGY

9.1 The Network Manager, the Compliance Officer and the Data Protection Officer must be consulted before the acquisition of any new technology:

- To consider compatibility,
- To ensure data protection principles are adhered to,
- To enable a risk assessment to be completed,
- The use of smart phones by students will be reviewed regularly in the light of emerging technology and the impact of phone usage on the health and well-being of students.

10 E-SAFETY PROMOTION AND EDUCATION

10.1 This will be managed by the person appointed by the Principal.

10.2 Promoting e-safety consists of:

- Fostering an open environment in which students and staff can ask questions and consider the benefits and dangers of the online world,
- Promoting e-safety awareness,
- Ensuring that monitoring of use of school systems takes place and has impact.

10.3 Education comprises:

- Research and Development of age-appropriate materials for delivery to students to support all parts of the curriculum (not just Computer Science lessons),
- Ensuring that this curriculum is inclusive,
- Ensuring that the materials can be delivered by a non-specialist,
- Providing materials to staff so that they can support anyone who has an e-safety problem,
- Producing material which is presented on the Trust's website for parents/carers to access,
- Ensuring that the material produced is regularly reviewed and current.

11 AUTHOR

11.1 The author of this policy is the Compliance Officer. They should be contacted for any points of clarification or suggested future amendments.

12 VERSION CONTROL

Policy Number	COMDA-06
Policy Name	E-Safety
Version Number	02
Publication Method	External A copy must be made available in U:\Staff Information\Policies\COMmunications and DAta Policies
Approved by	Full Trust Board
Date of Approval	October 2023
Key changes since previous version	1. Stating the two methods which are being used to improve the e-safety of the Trust and those who access its systems. 2. Extending the use of technology beyond to the wider considerations.
Next review date	September 2024