Birmingham Ormiston Academy

imagine everything

BOA

E-safety Policy

Date of Issue: January 2016

Updated: 09.09.16

Date of Review: September 2017

CONTENTS **PAGE**

1 INTRODUCTION

The internet provides a vast range of invaluable tools and opportunities which can be used to enrich and enhance learning experiences, and to communicate efficiently. Children and young people engage with the internet every day, using a variety of platforms and devices both inside and outside of the academy, so it is important to recognise the role of the academy in educating and supporting them in being safe whilst doing so.

BOA intends to provide an outstanding learning environment, where student and staff access to the internet is managed in such a way as to keep access as open as possible, promoting experimentation with new technologies and tools, whilst at the same time ensuring that we protect our students and staff from harm.

2 SCOPE

2.1 This policy defines outstanding practice as identified in the latest OFSTED inspection framework.

2.2 This policy identifies e-safety risks as identified in the Dfe KCSE guidance, Ofsted's 3Cs (Content, Contact, Conduct), and Becta's Safeguarding Children in a Digital World advice.

2.3 This policy details key strategies and measures taken to minimise e-Safety risks.

2.4 This policy details key strategies for educating students, staff and parents to ensure they are empowered to recognise and manage risk, ensuring that children use new technologies safely and responsibly both at home and the academy.

2.5 This policy specifies the ways by which e-safety concerns are monitored, reported, logged by students, staff and parents.

2.6 This policy identifies clear and transparent procedures to audit, measure, evaluate and improve the impact of e-safety at the academy.

2.7 This policy details the strategy by which the academy will transition from locked down systems to managed e-safety systems.

2.8 The technologies covered by this policy include, but not exclusively:

- All websites, chat rooms, instant messaging and social networking sites
- Virtual Learning Environments (VLE) e.g. RealSmart and Googledrive
- E-mail (both Academy and personal accounts)
- SMS, MMS and other forms of text messaging
- Blogs/Wikis
- SIMS or any proprietary student tracking software
- Pod/Vodcasting
- Video, audio and music downloading
- Telephony (for example Skype, web conferencing etc.)
- New and emerging technologies not covered above

2.9 This policy should be read in conjunction with the policies and procedures listed in section 9

3 OFSTED FRAMEWORK AND GUIDANCE

3.1 Ofsted have defined e-safety thus:

In the context of an inspection e-safety may be described as the academy's ability to protect and educate pupils and staff in their use of technology and to have the appropriate mechanisms to intervene and support any incident where appropriate

3.2 E-safety will be inspected in relation to the following areas:

- The behaviour and safety of pupils at the academy
- The quality of leadership in, and management of, the academy

3.3 Ofsted have identified three areas of e-safety risk in relation to pupils:

- Being exposed to illegal, inappropriate or harmful material
- Being subjected to harmful online interaction with other users
- Personal online behaviour that increases the likelihood of, or causes, harm.

3.4 An outstanding academy will demonstrate that:

All groups of pupils feel safe at the academy and at alternative provision placements at all times. They understand very clearly what constitutes unsafe situations and are highly aware of how to keep themselves and others safe, including in relation to e-safety.

3.5 Ofsted will examine how the academy:

- Audits the training needs of all staff and provides training to improve their knowledge of and expertise in the safe and appropriate use of new technologies.
- Works closely with all families to help them ensure that their children use new technologies safely and responsibly both at home and the academy.
- Uses pupils' and families' views more often to develop e-safety strategies
- Manages the transition from locked down systems to more managed systems to help pupils understand how to manage risk; to provide them with richer learning experiences; and to bridge the gap between systems at the academy and the more open systems outside of the academy

3.6 Key features of good and outstanding practice:

- All staff understand e-safety issues, e-safety is an academy priority. The academy has, or is working towards an e-safety Mark. Training in e-safety is audited and provided to all staff. A number of members of staff have received accredited e-safety training. pupils, parents, wider academy community stakeholders and governors all contribute to build a fluid and constantly evolving e-safety policy.
- Clear and transparent procedures exist for monitoring, logging, reporting incidents, evaluating, improving and measuring the impact of e-safety. All staff, parents, pupils, contractors and governors know how to report an e-safety incident.

4 E-SAFETY RISKS

As identified in Becta's Safeguarding Children in a Digital World advice and the UK Council for Child Internet Safety's report on Children's online risks and safety:

The internet and the increasing prevalence of new technologies have resulted in emerging risks associated with privacy invasion, cybercrime, cyber-bullying and educational misconduct through for example, but not exclusively:

- **Lack of understanding of the risks attached to sharing personal information** (e.g. sharing/distribution of personal images without an individual's consent or knowledge)
- **Access to illegal, harmful or inappropriate images or other content** (e.g. child abuse)
- **Access to socially unacceptable material** (e.g. extreme violence)
- **Access to unsuitable video/internet games, films or other media** (e.g pornography)
- **Inappropriate communication/contact with others, including strangers**
- **Cyberbullying**
- **The risk of being subject to grooming/sexual exploitation by those with whom contact is made on the internet**
- **Inability to evaluate the quality, accuracy and relevance of information on the internet** (e.g. access to age-inappropriate material)
- **Risks associated with social networking**
- **Plagiarism and copyright infringement**
- **Commercial and financial scamming schemes**
- **Illegal downloading of music or video files**
- **Radicalisation** (More recently, there has been an increase in groups and individuals trying to approach young people to recruit them for political or religious ideas. This is known as online radicalisation and can be described as; *"The actions of an individual or group who use the Internet and digital technology to groom a young person into following their extremist ideas.")*

5 STRATEGIES AND MEASURES TO MINIMISE RISK

5.1 Filtering web access.

5.1.1 In accordance with Dfe guidelines and recommendations, the Academy with make use of filtering software (Smoothwall and Impero) to block access to:

- Websites that host illegal, harmful or inappropriate images or other content (e.g. child abuse)
- Websites that host socially unacceptable material (e.g. extreme violence)
- Websites that host unsuitable video/internet games, films or other media (e.g pornography)
- Websites which enable/encourage plagiarism and copyright infringement
- Websites that actively host or promote commercial and financial scamming schemes
- Websites that promote or host illegal downloading of music or video files
- Social networking sites where "trolling" is encouraged, users can post anonymous comments, or there is a history of the platform being used to groom, exploit or radicalise children and young people.
- Any other website or platform which is deemed to pose a severe risk to student safety.

5.1.2 Persons Responsible:

- IT Support and Services Manager and Gaia Network Support Technician (Network Manager)
- Teaching staff will be responsible for managing student web access in classrooms beyond those categories listed above, making use of localised classroom management/filtering software.

5.2 Monitoring and reporting on web access

5.2.1 Website access and" trigger words" will be monitored at all times using filtering/monitoring software and reports generated and examined on a regular basis. This will enable informed decisions to be made as to whether additional sites need to be added to an exclusions list, and to flag users who may be at risk of harm or breaching policy.

5.2.2 Attempts to access material in blocked categories [5.1] and/or outside acceptable parameters detailed in the Computer and Internet Acceptable Use Policy (Apprendix A), will be reported immediately/automatically via the Smoothwall application, scrutinised by the IT Support and Services manager/AP for Digital Arts and New technologies and if appropriate referred on in accordance with the e-safety reporting procedure detailed in section 5.5.

5.2.3 Web access reports are to be presented to the Assistant Principal of Digital Arts, New Technology and IT weekly.

5.2.4 Web access summary reports are to be presented to SLT on a half-termly basis for review.

5.2.5 Persons Responsible: IT Support and Services Manager, Gaia Network Support Technician (Network Manager), All teachers, SLT.

5.3 IT Acceptable Use Policy (ICT, Internet, Social Media) [Appendix A]

All staff and students will be required to adhere to the BOA Computer and Internet Acceptable Use Policy. The Acceptable Computer Use and Internet Policy helps to protect students, staff and the academy by clearly stating what use of computer resources is acceptable and what is not. BOA expects all students to adhere to this policy for acceptable use of the equipment to maintain a positive learning environment.

All staff and students will be required to adhere to the requirements in the Acceptable Use policy regarding the safe and appropriate use of Social Media. The BOA approach to Social Media is designed to ensure that students and staff members use social media safely and responsibly in order to protect themselves, the confidentiality of students and

staff and the reputation of the Academy. Use of social media sites associated with the academy will be closely monitored. Staff must request permission to set up Social media sites for academy business. No site will be authorised without careful consideration and full disclosure of administrative access details.

5.4 Reporting E-Safety Concerns

5.5.1 All concerns/incidents regarding e-safety should be directed in the first instance to the Assistant Principal Pastoral Care and Guidance (DSL)(Designated Safeguarding Lead) in accordance with the safeguarding policy and reporting procedure.

5.5.2 In addition an E-safety reporting button and Child Exploitation and Online Protection (CEOP) reporting button are available on the BOA academy website, Old Rep Theatre Website, VLE and any other emerging web based technologies made available to students and staff.

5.5.3 Should the Designated Safeguarding Lead (DSL) feel the concern/incident warrants immediate action in the form of a web access lockdown (or similar), he/she will refer the case immediately to the IT Support and Services Manager who will implement the required safeguards.

5.5.4 Staff, students and parents will be provided with details of this procedure and methods by which to contact the DSL at induction and further training will be provided as and when deemed necessary.

5.5.5 Persons Responsible: All staff, Assistant Principal Pastoral Care and Guidance (DSL), IT Support and Services Manager

5.5 Educating Students

5.6.1 Students will be provided with information and training in regard to:

- BOA's E-safety Policy and Procedures
- BOA's Acceptable Use Policy
- What constitutes unsafe situations and how to keep themselves and others safe in relation to e-safety:
  - Cyber bullying
  - Sexting
  - Radicalisation
  - Social Media
  - Digital footprint
  - Reliability and validity
  - Protection of personal information
  - Meeting up with strangers
  - Privacy , phishing and commercial risks
- How to report a concern or incident
- How to identify and manage risk online
- How to contact key external online safety support agencies (eg.CEOP)

5.5.2 The platforms from which this training will be provided include but are not limited to:

- E-safety Support – Online Training Module (Approved CPD Cert)
- Induction
- Tutorials
- Learning to learn programme
- Website and VLE E-safety information page
- Safer Internet Day events

- Voice of BOA events
- Assemblies
- Personalised support (students who require extra guidance)
- Embedded in curriculum (where relevant)
- Independent learning (e.g: E-learning)

5.5.3 Responsible Persons: Assistant Principal: Learning and Personal Development/ Assistant Principal: Pastoral care and Guidance. Assistant Principal: Digital Arts and New Technologies.

5.6 Educating Staff

5.6.1 Staff will be provided with information and training in regard to:

- BOA's E-safety policy and procedures
- BOA's Acceptable Use Policy
- BOA's Safeguarding policy and procedures
- BOA's ICT Whole School Policy
- What constitutes unsafe situations and how to keep themselves and their learners safe in relation to e-safety.
- How to raise learners' awareness of e-safety
- How to report a concern or incident
- How to identify and manage risk online
- How to contact key external online safety support agencies (eg.CEOP)

5.6.2 The platforms from which this training will be provided include but are not limited to:

- E-safety Support – Online Training Module (Approved CPD Cert)
- Staff Induction
- Website and VLE e-safety information page
- Staff development (e.g: E-learning, inset days)

5.6.3 Responsible Persons: Assistant Principal Learning and Personal Development. Assistant Principal Digital Arts, New technologies, ICT. Assistant Principal Pastoral care and Guidance.

5.7 Educating Parents/Guardians

5.7.1 Parents/Guardians will be provided with information and training in regard to:

- BOA's e-safety policy and procedures
- BOA's Computer and Internet acceptable use policy
- What constitutes unsafe situations and how to keep their children safe in relation to e-safety at home
- How to report a concern or incident
- How to identify and manage risk online
- How to contact key external online safety support agencies (eg.CEOP)

5.7.2 The platforms from which this training will provided include but are not limited to:

- Website e-safety page
- Parents' Evening presentations
- Safer Internet Day correspondence
- Distance e-learning resources (E-safety Support – Online Training Module (Approved CPD Cert))

5.8.3 Responsible Persons: Assistant Principal Digital Arts, New technologies, ICT. Assistant Principal Pastoral care and Guidance.

5.8 Seeking the views of parents, student and staff

5.8.1 Steps will be taken to seek, collate and review the views of parents, students and staff in relation to e-safety and the effectiveness of the safeguards the academy has put into place.

Forums from which these views will be sought will include but not limited to:

- Parent's evenings
- Open evenings
- Learner voice events
- Tutorials
- Staff development days
- Online/Offline surveys

5.8.2 Upon collation of feedback from the above parties/events, the Assistant Principal for New Technologies, Digital Arts and IT will review the Academy E-safety policy and procedures, making amendments when deemed necessary.

5.8.3 Responsible: Assistant Principal for New Technologies, Digital Arts and IT

5.9 Continuous review of new and emerging technologies

5.9.1 On an ongoing basis the IT Support and Services Manager will work closely with the Assistant Principal for New Technologies, Digital Arts and IT to review new and emerging technologies, assessing associated risks and adapting safeguards in place at the academy as required.

5.9.2 Responsible: IT Support and Services Manager, Assistant Principal for New Technologies, Digital Arts and IT

5.10 E-safety audit and improvement planning

5.10.1 On a day to day basis monitoring, impact analysis and development is embedded in e-safety procedures.

5.10.2 In addition an annual e-safety audit will be completed by the Assistant Principal for New Technologies, Digital Arts and IT. The objectives of the audit is to:

- Measure the effectiveness/impact of policy and procedures
- Risk assess the potential impact of new developments in technology
- Specify a development/improvement plan

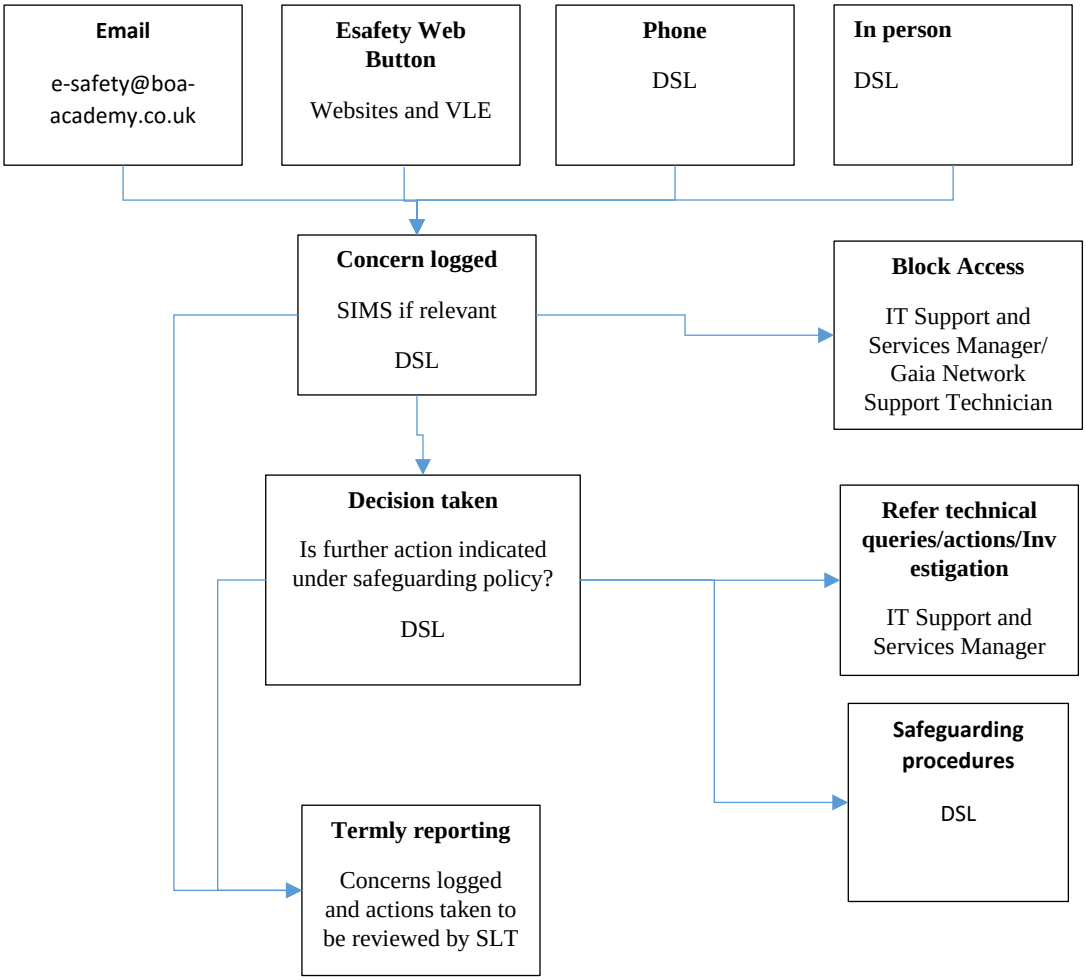
5.10.3 The information examined to complete the e-safety audit includes (although not limited to) the following:

- Parent /Student Feedback summary report
- User access data (flagged/non flagged) summary report

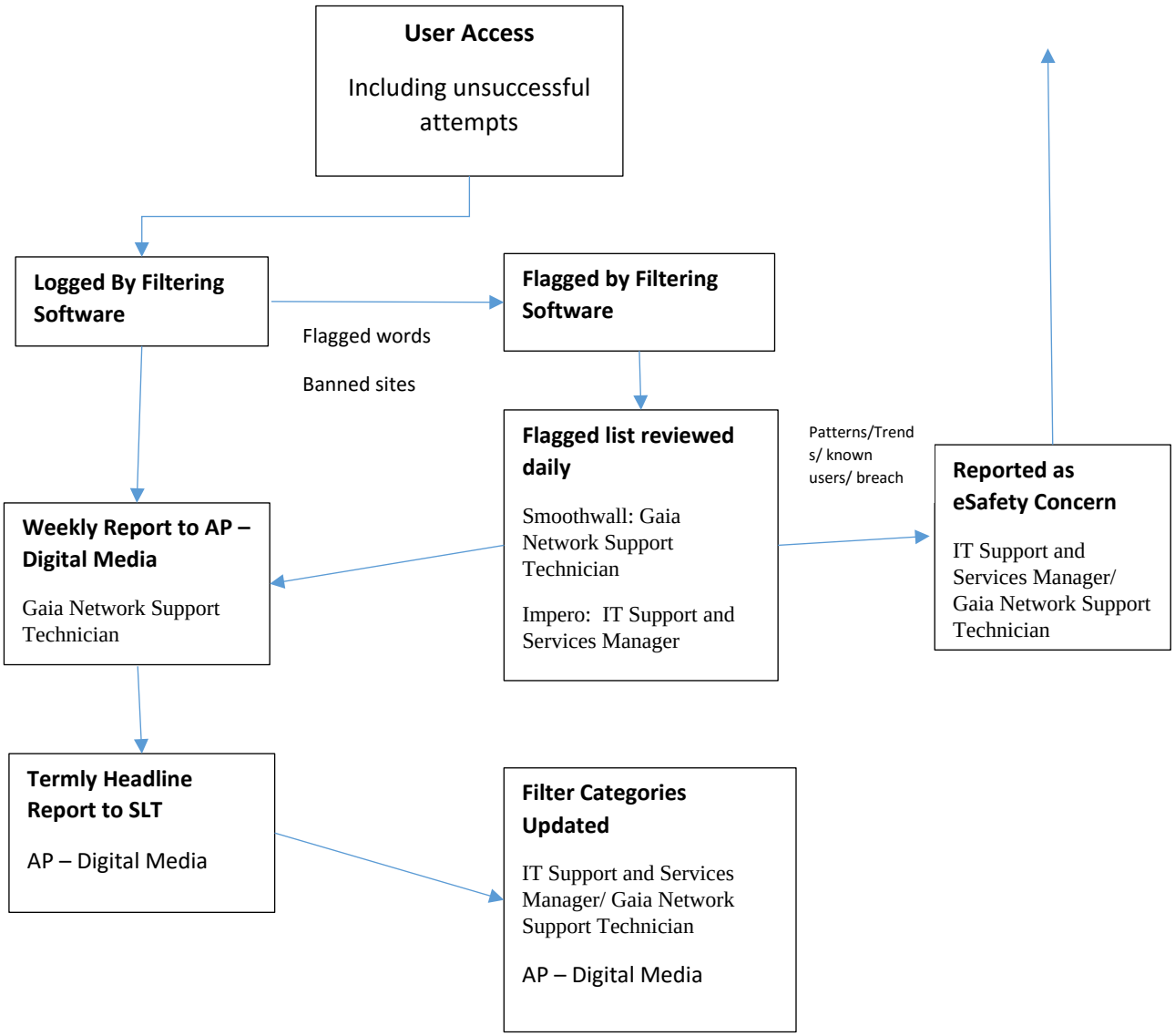
- E-safety concern summary report
- E-safety related safeguarding case-studies

6 PROCEDURES

6.1 Monitoring, reporting, logging e-safety concerns



6.2 **Web access monitoring and reporting**



7. TRANSITION TO MANAGED SYSTEMS

In January 2016 BOA Academy began the transition from locked down to managed systems.

The following is an overview of key stages in the planned transition process and progress as of 09.09.16:

1516 ACADEMY TERM 3		
Refine infrastructure and identify capabilities of present equipment and software. Implement *Smoothwall* filtering and I*mpero* monitoring tools.	IT Support and Services Manager/ Gaia Network Support Technician	✓
Develop further training resources for Students, Staff and Parents	AP – Digital Media	✓
Risk assess web categories in software filtering system	AP – Digital Media	✓
1516 ACADEMY TERM 4		
Provide updated training for Students, Staff and Parents	AP – Digital Media	✓
Roll back filtering from low risk web category (e.g. entertainment review sites)	Gaia Network Support Technician	✓
Report back on effectiveness of monitoring and reporting systems	IT Support and Services Manager	✓
Seek staff, student and parental feedback	AP – Digital Media	✓
Make amendments to systems as required	IT Support and Services Manager/ Gaia Network Support Technician	✓
Provide additional training as required	AP – Digital Media	✓
1516 ACADEMY TERM 5		
Roll back filtering from medium risk web category as pilot (e.g. online games for Games Design students, Pintrest for Art Students)	Gaia Network Support Technician	✓
Report back on effectiveness of monitoring and reporting systems	IT Support and Services Manager	✓
Seek staff, student and parental feedback	AP – Digital Media	✓
Make amendments to systems as required	IT Support and Services Manager/ Gaia Network Support Technician	✓
Provide additional training as required	AP – Digital Media	✓
1516 ACADEMY TERM 6		
E-safety Audit point July 16	AP – Digital Media	✓
1617 ACADEMY TERM 1		
E-safety training update for all staff	AP – Digital Media	✓
E-safety training update for all students and roll-out of revised Acceptable Use Policy	AP – Digital Media	
1617 ACADEMY TERM 2		
Training focus on social media and remote communication Further differentiate filter blocks by pathway and age group	AP – Digital Media IT Support and Services Manager/ Gaia Network Support Technician	
1617 ACADEMY TERM 3		
Review of effectiveness of Google classroom as communication tool	AP – Digital Media	
1617 ACADEMY TERM 4		
Training focus on Radicalisation (update)	AP – Digital Media	
1617 ACADEMY TERM 5		
Review Filter Categories	AP – Digital Media IT Support and Services Manager/ Gaia Network Support Technician	
1617 ACADEMY TERM 6		
E-safety Audit Point	AP – Digital Media	

8. BREACHES OF POLICY

Breaches of the e-safety policy and procedures will be dealt with in accordance with the disciplinary procedure as identified in the staff handbook.

9. RELATED POLICIES

Appendix 1: Safeguarding Policy

Appendix 2: Acceptable Use Policy – Pupils and Parents

Appendix 3: Acceptable Use Policy - Staff