Avonbourne Girls' Academy
The best in everyone™
Part of United Learning

Avonbourne Boys' Academy
The best in everyone™
Part of United Learning

DRAFT

Online and E-Safety Policy

September 2019

Background / Rationale

Avonbourne Academies believes that online safety (e-Safety) is an essential element of safeguarding children and adults in the digital world, when using technology such as computers, mobile phones or games consoles.

The Academies identifies that the internet and information communication technologies are an important part of everyday life so children must be supported to be able to learn how to develop strategies to manage and respond to risk so they can be empowered to build resilience online. Avonbourne Academies has a duty to provide the school community with quality Internet access to raise education standards, promote pupil achievement, support professional work of staff and enhance the school's management functions. The Academies also identifies that with this there is a clear duty to ensure that children are protected from potential harm online.

The use of these new technologies can put young people at risk within and outside the Academies. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person
- Many of these risks reflect situations in the off-line world and it is essential that this E-Safety Policy is used in conjunction with other Academies Policies, including the Acceptable Use Policy, Behaviour Policy and Safeguarding Policy.

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build students' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

Scope of the Policy

The purpose of Avonbourne Academies's online safety policy is to clearly identify the key principles expected of all members of the community with regards to the safe and responsible use technology to ensure that Academies is a safe and secure environment for all students and staff.

This policy applies to all staff including the governing body, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for or provide services on behalf of the school (collectively referred to as 'staff' in this policy) as well as children and parents/carers.

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students when they are off the Academies 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

Academies, but is linked to membership of the Academies. The Academies will deal with such incidents within this policy and associated behaviour policies and will, where known, inform parents/carers of incidents of inappropriate e-safety behaviour that take place out of the Academies.

The Academies will monitor the impact of the policy using:

- Logs of reported incidents.
- Internet provider monitoring logs of internet activity (including sites visited).
- Internal monitoring data for network activity.
- Safeguarding Team monitoring and follow-up of issues identified by Smoothwall (internal daily monitoring system).
- Surveys / questionnaires – students; parents/cares; staff.

Roles and Responsibilities

The following section outlines the roles and responsibilities for e-safety of individuals and groups within the Academies:

Governors:

- Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out through regular reporting to Governor Committee by the Designated Senior Person for Safeguarding and Child Protection.

Executive Headteacher / Senior Leaders:

- The Executive Headteacher responsible for ensuring the safety (including e-safety) of members of the Academies community, through the day to day responsibility for e-safety will be delegated to the Designated Lead for Safeguarding and/or Online Safety Lead.
- The Designated Lead for Safeguarding and/or Online Safety Lead will liaise with the Academies Network supervisor and/or ICT staff in order to monitor all aspects of E-Safety.
- The Designated Lead for Safeguarding will set out procedures to be followed in the event of a serious e-safety allegation being made against a member of staff in line with the Academies Acceptable User Policy and Safeguarding Policy.

The Designated Lead for Safeguarding/Online Safety Lead:

- Liaise with relevant staff.
- Have a leading role in establishing and reviewing the Academies E-Safety policy and other relevant 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.
- Liaise with the Academies ICT teaching and technical staff.
- Receive reports of e-safety incidents and ensure a member of the safeguarding team reviews and allocates relevant members of the team to follow-up any concerns.
- Ensure online safety concerns are logged MyConcern on with appropriate action.
- Ensure Internet filtering reports that identify behaviour which might indicate safeguarding issues or inappropriate behaviours are logged as appropriate and referred to Behaviour Lead.
- Meets regularly with the Safeguarding Governors to discuss current issues, review incident logs and filtering / change control logs.
- Attends relevant Governor meetings.

Network Manager / Technical Staff

The Network Manager, ICT Support Staff are responsible for ensuring:

- That the Academies ICT infrastructure is secure and is not open to misuse or malicious attack.
- That the Academies meet appropriate e-safety technical requirements to fulfil the Acceptable Use Policy.
- That users may only access the Academies networks through a properly enforced password protection system, in which passwords are encouraged to be regularly changed.
- That the filtering software provider is informed of issues relating to the filtering they apply
- That they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant.
- That the use of the network / remote access / email is regularly monitored in order that any misuse or attempted misuse can be reported to the Designated Lead for Safeguarding for investigation/Principal and/or Executive Headteacher and actioned.
- That monitoring software / systems are implemented and updated.

Teaching and Support Staff

Teaching and Support Staff are responsible for ensuring that:

- They have an up to date awareness of e-safety matters and of the current Academies E-Safety policy and practices.
- They have read, understood and signed off the Academies Staff Acceptable Use Policy.
- They report any suspected misuse of problem to the Designated Lead for Safeguarding, Network Supervisor and Principal and/or Executive Headteacher as appropriate.
- Digital communications with students (email/ google classroom) should be on a professional level and only carried out using official Academies systems.
- E-safety issues are embedded in the curriculum and other Academies activities.
- Students understand and follow the Academies e-safety and Acceptable Use Policy.
- Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- They monitor ICT activity in lessons, extra-curricular and extended Academies activities.
- They are aware of e-safety issues related to the use of mobile phones, cameras and hand-held devices and that they monitor their use and implement current Academies policies with regard to these devices.
- In lessons where internet use is pre-planned students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Students

- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Will be expected to know and understand Academies policies on the use of mobile phones, digital cameras and hand-held devices. They should also know and understand Academies policies on the taking / use of images and on cyberbullying.
- Should understand the importance of adopting good e-safety practice when using digital technologies out of the Academies and realise that the Academies E-Safety Policy covers their actions whilst outside of the Academies, if related to their membership of the Academies.

Parents / Carers

Parents / carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The Academies

will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website / local e-safety campaigns / literature.

Parents and carers will be responsible for:

- Endorsing (by signature) the Student Acceptable Use Policy.
- Accessing the Academies website / on-line student systems / student records in accordance with the relevant Academies Acceptable Use Policy.

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in e-safety is therefore an essential part of the Academies e-safety provision.

Children and young people need the help and support of the Academies to recognise and avoid e-safety risks and build their resilience.

E-Safety education will be provided in the following ways:

- Through a planned e-safety programme through SMSC and other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in and outside school.
- Through key e-safety messages reinforced as part of a planned programme of assemblies and tutor activities.
- Students should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Students should be helped to understand the Acceptable Use Policy and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside of the Academies.
- Students will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Staff should act as good role models in their use of ICT, the internet and mobile devices.

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide" – Byron Report.

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

- Letters, newsletters and web site
- Parents consultation and information evenings

All staff will receive e-safety training in order to understand their responsibilities, as outlined in the policy. Training may take the format of:

- A planned programme of formal e-safety training.
- Regular updates will be provided to all staff through ICT staff. Online Safety Lead or the Designated Lead for Safeguarding.

Governors will be invited to take part in e-safety training through:

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

Curriculum

E-Safety should be a focus in all areas of the curriculum and should reinforce E-Safety messages in the use of ICT across the curriculum

- In lessons where internet use is pre-planned, it is best practice that students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where students are permitted to freely search the internet, e.g. using search engines, staff should be 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 (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the IT team can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.
- Students should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

Use of digital and video images – photographic, video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff and students need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. The Academies will inform and educate users about these risks and will implement systems to reduce the likelihood of the potential for harm:

When using digital images, staff should inform and educate students about the rules and risks associated with the taking, use, sharing, publication and distribution of images.

- Staff are allowed to take digital / video images to support educational aims, but must follow Images of Children protocol concerning the sharing, distribution and publication of those images. Those images should only be taken on Academies equipment, the personal equipment of staff should not be used for such purposes unless explicit permission has been given by the Principal and/or Executive Headteacher – see Safeguarding Policy for further details.
- Care should be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals of the Academies into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with Images of Children protocol.
- Students' full names will not be used anywhere on a website or blog, particularly in association with photographs unless complying with Images of Children protocol.
- Written permission from parents or carers will be obtained before photographs of students are published on the Academies websites.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly 'logged-off' at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system:

- The data must be encrypted and password protected.
- The device must be password protected (many memory sticks / cards and other mobile devices cannot be password protected).
- The device must offer approved virus and malware checking software.
- The data must be securely deleted from the device, in line with Academies policy once it has been transferred or its use is complete.

Communications

When using communication technologies, the Academies will consider the following as good practice:

- The official Academies email service may be regarded as safe and secure and is monitored.
- Users need to be aware that email communications are monitored.
- Users must immediately report the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and students or parents / carers (email) must be professional in tone and content. These communications may only take place on official (monitored) Academies systems. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications.
- Students should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the Academies website and only official email addresses should be used to identify members of staff.

Responding to incidents of misuse

It is hoped that all members of the Academies community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless, irresponsible or, very rarely, through deliberate misuse.

Any breech of the above by students will be sanctioned under our behaviour system rules. We reserve the right to remove a student's access to the internet for continued violations of the Acceptable Use Policy and E-Safety Policy. Any internet search of concern is referred to our safeguarding team. The Academies will inform parents/carers of any incidents of concern as and when required.

The Designated Safeguarding Lead (DSL) will be informed of any online safety (e-Safety) incidents involving child protection concerns, which will then be recorded. The Designated Safeguarding Lead (DSL) will ensure that online safety concerns are escalated and reported to the United Learning Designated Safeguarding Officer and relevant agencies in line with the Local Safeguarding Children Board thresholds and procedures.

Examples of misuse include:

- Child sexual abuse images
- Adult material which potentially breaches the Obscene Publications Act
- Criminally racist material
- Other criminal conduct, activity or materials

Any complaint about staff misuse will be referred to Executive Headteacher. Any allegations against a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer). Incidents of misuse will be dealt with in line with either the LA or United Learning Safeguarding and Disciplinary procedures. Staff should refer to the Whistleblowing Policy procedure if appropriate.

Appendix A

Online Safety (e-Safety) Contacts and Reference

National Links and Resources

Action Fraud: www.actionfraud.police.uk

BBC WebWise: www.bbc.co.uk/webwise

CEOP (Child Exploitation and Online Protection Centre): www.ceop.police.uk

ChildLine: www.childline.org.uk

Childnet: www.childnet.com

Get Safe Online: www.getsafeonline.org

Internet Matters: www.internetmatters.org

Internet Watch Foundation (IWF): www.iwf.org.uk

Lucy Faithfull Foundation: www.lucyfaithfull.org

Know the Net: www.knowthenet.org.uk

Net Aware: www.net-aware.org.uk

NSPCC: www.nspcc.org.uk/onlinesafety

Parent Port: www.parentport.org.uk

Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline

The Marie Collins Foundation: http://www.mariecollinsfoundation.org.uk/

Think U Know: www.thinkuknow.co.uk

Virtual Global Taskforce: www.virtualglobaltaskforce.com

UK Safer Internet Centre: www.saferinternet.org.uk

360 Safe Self-Review tool for schools: https://360safe.org.uk/

The School Online Safety Lead (e-Safety) is:

The School Designated Safeguarding Lead (DSL) is: Natasha England

Policy approved by Head Teacher: …… Date: ……

Policy approved by Governing Body: …….. (Chair of Governors) Date: ……

The date for the next policy review is: September 2019