Ambitious about Autism
E-safety policy
2017

Contents:

Schedule for Development/Monitoring/Review

This e-safety policy was approved by the Governing Body and Board of

trustees: DATE.

Monitoring of the E-Safety Policy will take place at regular intervals.

The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be January 2018.

Ambitious about Autism will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity
- Weekly website access monitoring

Scope of the Policy

This policy applies to Ambitious about Autism (AAA), which includes the Charity, Ambitious College and TreeHouse School and all staff, pupils, volunteers, parents/carers, visitors, community users, contractors and consultants, who have access to and are users of Ambitious about Autism ICT systems and data, both in and outside of the premises.

This E-Safety policy recognises the commitment of Ambitious about Autism to e-Safety and acknowledges its part in the AAA's overall safeguarding policies and procedures. It shows our commitment to meeting the requirement to keep all members safe when using technology. We believe the whole AAA community can benefit from the opportunities provided by the Internet and other technologies used in everyday life. The e-Safety policy supports this by identifying the risks and the mitigating actions we are taking to avoid them. It shows our commitment to developing a set of safe and responsible behaviours that will enable us to reduce the risks whilst continuing to benefit from the opportunities. It ensures that all members of the AAA community are aware that unlawful or unsafe behaviour is unacceptable and that, where necessary disciplinary or legal action will be taken.

This policy explains how Ambitious about Autism's ICT resources are to be used and what actions are not allowed. While this policy is as complete as possible, no policy can cover every situation. Questions as to what is deemed acceptable use can be directed to the E-safety coordinator, Executive Leadership Team (ELT), Senior Leadership Teams.

Other policies to be referred to:

- Data Security Policy
- Data Protection Policy
- Confidentiality Policy
- Disciplinary Policy and Procedure
- Grievance Policy and Procedure
- Child Safeguarding and Protection Policy and Procedure
- Adult Safeguarding and Protection Policy and Procedure
- Preventing Extremism and Radicalisation Policy

The use of computers and network resources is subject to meeting all relevant UK legislation including, but not limited to:

- Computer Misuse Act
- Regulations of Investigative Powers Act (RIPA)
- Data Protection Act
- Obscene Publications Act
- Copyrights, Design and Patents Act
- Communications Act
- Computer Copyright Software Amendment Act

Roles and Responsibilities

The following section outlines the e-safety roles and responsibilities of individuals and groups within AAA.

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 by the Governors receiving information about e-safety incidents from the AAA/Principal/Headteacher reports.

Principal, Headteacher and Senior Leaders:

- Has a duty of care for ensuring the safety (including e-safety) of members of the college and school community, though the day to day responsibility for e-safety will be delegated to the E-Safety Co-coordinator.
- Should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.
- Are responsible for ensuring that the E-Safety Coordinator/Designated Senior Person and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- Will ensure that there is a system in place to allow for monitoring and support of those in AAA who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

Head of IT:

The Head of IT is responsible for ensuring:

- day to day responsibility and has a leading role in establishing and reviewing the AAA 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 Local Authority/relevant body where required
- liaises with AAA technical staff
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- reports any e-safety incidents to the Principal, Headteacher or Senior leader as required
- That AAA's technical infrastructure is secure and is not open to misuse or malicious attack.

- That the college and school meet required e-safety technical requirements and any Local Authority/other relevant body E-Safety Policy/Guidance that may apply.
- That users may only access the networks and devices through an enforced password protection rule, in which passwords are regularly changed.
- 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/internet/remote access and email is regularly monitored in order that any misuse/attempted misuse can be reported to the Principal or Headteacher, E-Safety Coordinator, Senior Leader for investigation/action/sanction.
- That monitoring software/systems are implemented and updated regularly.

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 AAA e-safety policy and practices.
- They have read, understood and signed the Staff Acceptable Use Agreement.
- They report any suspected misuse or problem to the Principal/Headteacher/Head of IT/ Senior Leader for investigation/action/sanction.
- All digital communications with pupils/parents/carers should be on a professional level and only carried out using official AAA systems.
- E-safety issues are embedded in all aspects of the curriculum and other activities.
- Learners and pupils understand and follow the e-safety and acceptable use agreements.
- Learners and pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- They monitor the use of digital technologies, mobile devices, cameras etc. at work,in lessons and other college and school activities (where allowed) and implement current policies with regard to these devices.
- In lessons where internet use is pre-planned, learners and pupils 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.

Safeguarding Designated Person:

The Safeguarding Designated Person should be trained in e-safety issues and be aware of the potential for serious safeguarding issues to arise from:

- sharing of personal data
- access to illegal/inappropriate materials
- inappropriate on-line contact with adults/strangers
- potential or actual incidents of grooming
- cyber-bullying

Parents/Carers:

Parents/carers play a crucial role in ensuring that their children or young adults understand the need to use the internet/mobile devices in an appropriate way. The college/school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national/local e-safety campaigns/literature. Parents and carers will be encouraged to support the college/school in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- Digital and video images taken at school events.
- their children's personal devices in the school (where this is allowed)

Policy Statements

Education – learners/pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating learners and pupils to take a responsible approach. The education of learners and pupils in e-safety is therefore an essential part of the e-safety provision. Children and young adults need the help and support of the organisation to recognise and avoid e-safety risks and build their resilience.

E-Safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum. The e-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned e-safety curriculum should be provided as part of ICT or other lessons and should be regularly revisited.
- Key e-safety messages should be reinforced as part of a planned programme of training activities.
- Learners/Pupils 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.
- Learners/Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Learners/Pupils should be helped to understand and be encouraged to adopt safe and responsible use both within and outside the college and school
- Staff should act as good role models in their use of digital technologies the internet and mobile devices
- In lessons where internet use is pre-planned, it is best practice that learners/pupils 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 learners/pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- Any request to block or unblock an internet site, should be recorded, with clear reasons for the need.

Education – parents/carers:

Parents/carers play an essential role in the education of their children and in the monitoring/regulation of their children's on-line behaviours. Parents may underestimate how often children and young adults come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

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

- Curriculum activities
- Letters, newsletters, website
- Parents/Carers evenings/sessions
- High profile events/campaigns egg Safer Internet Day

Education & Training – Staff/Volunteers:

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- 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.
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the AAA e-safety policy and Acceptable Use Agreements.
- The Head of IT will receive regular updates by reviewing guidance documents released by relevant organisations.
- This E-Safety policy and its updates will be presented to and discussed by staff in staff team meetings/INSET days, organisation meetings.
- The E-Safety Coordinator will provide advice/guidance/training to individuals as required.

Training – Governors:

Governors should take part in e-safety training/awareness sessions, with particular importance for those who are members of any sub-committee/group involved in technology/e-safety/health and safety or safeguarding. This may be offered in a number of ways:

- Attendance at training provided by Ambitious about Autism
- Participation in college/school training/information sessions for staff or parents.

Technical – infrastructure/equipment, filtering and monitoring:

AAA will be responsible for ensuring that the AAA infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

- AAA technical systems will be managed in ways that ensure that the AAA meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of AAA technical systems
- All users will have clearly defined access rights to AAA systems and devices.

- All users will be provided with a username and secure password. Users are responsible for the security of their username and password.
- AAA can provided enhanced/differentiated user-level filtering
- AAA technical staff regularly monitor and record the activity of users on the AAA systems and users are made aware of this in the Acceptable Use Agreement.
- An appropriate system is in place for users to report any actual/potential incident/security breach to the relevant person, as agreed.
- An agreed procedure is in place for the provision of temporary access of “guests” (e.g. trainee teachers, supply teachers, visitors, consultants and contractors) onto the AAA systems.
- Users are not permitted to download and or install applications (including executable or similar types) on to a AAA device or whilst using the AAA systems, without agreement from the IT department.
- Users may use the following types of removable media for the purposes detailed:
- CD/DVD – Playing original video material, original music and viewing data written to the media that is owned by the user (who has copyright ownership). The use of software written to writable versions of this media is strictly prohibited.
- USB Media (memory sticks) – this type of media can be used on AAA devices for transferring individual AAA work, this being data created by the user. The use of applications on this type of media is strictly prohibited.
- Other types of media that may exist may only be used for the movement of personal data where the user owns the copyright.

Bring Your Own Device (BYOD):

This provides advice and direction to AAA choosing to allow staff/learner/pupil use of personal mobile electronic devices at AAA to access the wireless networks.

Key Principles

- The term “device” in this policy refers to any personal mobile electronic device with the capability to connect to AAA Wi-Fi networks.
- AAA can allow staff/learner/pupils to bring their own devices to their premises and may provide access to AAA’s Wi-Fi networks.
- Use of devices at AAA will be governed by AAA developed guidelines and processes based on the Bring Your Own Device Implementation Guidelines and the needs of AAA.
- AAA will provide internet access through its wireless networks at no cost.
- Everyone is responsible for the care and maintenance of their devices including data protection and battery charging.
- AAA will not accept any liability for the theft, damage or loss of any device. Everyone who brings their own devices onto AAA sites do so at their own risk.
- AAA is not obliged to provide hardware or technical support for devices.
- Staff/Learner/pupils and their parents/carers must complete and return a signed agreement prior to connecting to AAA’s network.
- Where AAA has reasonable grounds to suspect that a device contains data which breaches the BYOD Agreement, they may confiscate the device for the purpose of

confirming the existence of the material. Depending on the nature of the material involved, further action may be taken including referral to the police. AAA disciplinary action may also be appropriate.

Learner/pupil BYOD Agreement

Prior to connecting their devices to the network, learner/pupils must return a signed agreement. This agreement must be signed by the parent/carer. It is important to ensure that learner/pupils are aware of and agree to their obligations under the learner/pupil Bring Your Own Device (BYOD) Policy and relevant policies, prior to using their own device on the AAA Wi-Fi networks. AAA staff should endeavour to ensure that the BYOD learner/pupil responsibilities are clearly understood by both learner/pupils and their parents or carers. The learner/pupil BYOD Agreement is a simple document with the purpose of acknowledging acceptance and agreement of the terms associated with AaA' s implementation of the Learner/pupil Bring Your Own Device (BYOD) Policy by both learner/pupils and parents/carers.

By accepting the terms, the learner/pupil and parents/carers acknowledge that they:

- Agree to comply with the conditions of this BYOD Policy.
- Understand that noncompliance may result in the learner/pupil being subject to school disciplinary action.

Learner/pupil BYOD agreements should be retained in print or electronic form for future access as required.

Cost to Learner/pupils

- Internet access through the AAA network will be provided at no cost to learner/pupils.
- Access to AAA resources such as shared drives, printers will be an AAA based decision.

Staff/Learner/pupil Responsibilities

Staff/Learner/pupils are solely responsible for the care and maintenance of their BYO devices. This includes but is not limited to:

- Managing battery life and regular charging of their device.
- Labelling their device for identification purposes.
- Purchasing and using device protective casing.
- Ensuring the device is safe and secure during travel to and from AAA and throughout the day.
- Maintaining up-to-date anti-virus software and operating system on their device.
- Taking insurance coverage of their own device to protect any accidental damage, theft or loss.
- Managing the battery life of their device and acknowledge that AAA is not responsible for charging their devices. ensure that their devices are fully charged before bringing them to AAA. AAA are not responsible for (or restricted from) providing facilities for charging their devices.
- must have a supported operating system and current antivirus software installed on their device and must continue to maintain the latest service packs, updates and antivirus definitions.
- Should not attach any AaA-owned equipment to their mobile devices without the permission of the principal or an AAA member of staff.
- Should clearly label their BYOD device for identification purposes.
- Labels should not be easily removable.
- Are responsible for securing and protecting their device at AAA. This includes protective/carry cases and exercising common sense when storing the device. AAA is not required to provide designated or secure storage locations.

- Responsible for ensuring the operating system and all software on their device is legally and appropriately licensed.

Damage and loss
Staff/Learner/pupils bring their devices to AAA at their own risk. In cases of malicious damage or theft of advice, existing AAA processes for damage to AAA or another person's property apply.
AAA will regularly review existing policies and processes to include BYO devices where appropriate e.g. Staff/Learner/pupil Welfare and Fair Discipline Code.

Technical Support
AAA staff are under no obligation to provide any technical support on either hardware or software.

Long-term care and support of BYODs
Staff/Learner/pupils are solely responsible for repair and maintenance of their own device. It is not AAA's responsibility.
Warranties: Staff/Learner/pupils should understand the limitations of the manufacturer's warranty on their BYO devices, both in duration and in coverage.

Insurance
BYO devices are not covered by AAA.

Acceptable use of BYO devices includes the below:

- Using AAA network services to seek out, access, store or send any material of an offensive, obscene, pornographic, threatening, abusive or defamatory nature is prohibited. Such use may result in legal and/or disciplinary action.
- shall not create, transmit, retransmit or participate in the circulation of content on their devices that attempts to undermine, hack or bypass any hardware and software security mechanisms that have been implemented AAA.
- must not copy, transmit or retransmit any material that is protected by copyright, without prior permission from the copyright owner.
- Mobile phone voice and text, SMS messaging or device instant messaging use by staff/learner/pupils during the working day is an AAA based decision.
- must not take photos or make video or audio recordings of any individual or group without the express written permission of each individual (including parent/carer consent for minors) being recorded and the permission of an appropriate staff member.
- shall comply with AAA policies concerning the use of BYODs at AAA while connected to AAA network.
- AAA retains the right to determine what is, and is not, appropriate use of BYODs device.
- The consequences of any breaches of this policy will be determined by AAA, in accordance with AAA's welfare and discipline policies.
- AAA adheres to the Data Protection Act principles.

Use of digital and video images:

The development of digital imaging technologies has created significant benefits to learning and the business, allowing staff, learners and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers, learners and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. AAA will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate learners/pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their young adult/children at the college/school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other learners or pupils in the digital/video images.
- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow college/school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on college/school equipment; the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital/video images that learners/pupils are appropriately dressed and are not participating in activities that might bring the individuals or AAA into disrepute.
- Learners/Pupils must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include staff/learners/pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Staff/Learners/Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of learners/pupils are published on the AAA websites.
- Learners/Pupil's work can only be published with the permission of the learner/pupil and parents or carers.

Data Protection:

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and the AaA Data Protection Policy.

All 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.

Communications:

A wide range of rapidly developing communications technologies has the potential to enhance learning.

When using communication technologies the AAA considers the following as good practice:

- The official AAA email service may be regarded as safe and secure.
- Users must immediately report the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and learners/pupils or parents/carers (email, chat etc.) must be professional in tone and content.
- Learners/Pupils should be taught about e-safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the AAA website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity:

AAA has a duty of care to provide a safe learning and working environment for learners/pupils and staff. AAA could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

AAA provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils/learners and staff through limiting access to personal information:

- Training to include: acceptable use; social media risks; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions.
- Risk assessment, including legal risk.

Staff should ensure that:

- No reference should be made in social media to learners, pupils, parents/carers or staff.
- They do not engage in online discussion on personal matters relating to members of the college or school community.
- Personal opinions should not be attributed to AAA, the college, school or local authority.

AAA’s use of social media for professional purposes will be checked regularly.

Appropriate and Inappropriate Use by Staff or Adults:

Staff members have access to the network so that they can obtain age appropriate resources for their classes and create folders for saving and managing resources. They have a password to access a filtered internet service and know that this should not be disclosed to anyone or leave a computer or other device unattended whilst they are logged in. All staff should receive a copy of the E-Safety Policy and a copy of the Acceptable Use Agreement, which they need to sign and return, to keep under file with a signed copy returned to the member of staff.

When accessing the Learning Platform from home, the same Acceptable Use Agreement will apply. The acceptable use should be similar for staff to that of the pupils and young adults so that an example of good practice can be established

In the Event of Inappropriate Use

If a member of staff is believed to misuse the internet or learning platform in an abusive or illegal manner, a report must be made to the Principal, Headteacher/Senior Leader immediately and then the Safeguarding Policy must be followed to deal with any misconduct and all appropriate authorities contacted.

Appropriate and Inappropriate Use by Pupils or Young Adults:

Acceptable Use Agreements detail how they are expected to use the internet and other technologies within AAA, including downloading or printing of any materials. The agreements are there for them to understand what is expected of their behaviour and attitude when using the internet. This will enable them to take responsibility for their own actions. For example, knowing what is polite to write in an e-mail to another person, or understanding what action to take should there be the rare occurrence of sighting unsuitable material. This also includes the deliberate searching for inappropriate materials and the consequences for doing so.

AAA should encourage parents/carers to support the agreement with their children or young adult. This can be shown by signing the Acceptable Use Agreements so that it is clear to the college/school setting or other establishment that the agreement are accepted by the parent/carer. This is also intended to provide support and information to parents/carers when children and young adults may be using the Internet beyond college/school education setting.

Further to this, it is hoped that parents/carers will add to future rule amendments or updates to ensure that they are appropriate to the technologies being used at that time and reflect any potential issues that parents/carers feel should be addressed, as appropriate.

The downloading of materials, for example, music files and photographs need to be appropriate and ‘fit for purpose’ based on research for work and be copyright free.

File-sharing via e-mail, weblogs or any other means online should be appropriate and be copyright free when using the learning platform in or beyond school/education setting or other establishment.

In the Event of Inappropriate Use

Should a learner/pupil be found to misuse the online facilities whilst on AAA premises, the following consequences should occur:

- may have a letter sent home to parents/carers explaining the misuse and resulting actions.
- Further misuse may result in further sanctions

- A letter may be sent to parents/carers outlining the breach in Policy where it is deemed that a learner/pupil have misused for peer on peer bullying against another learner/pupil or adult.

In the event that a learner/pupil **accidentally** accesses inappropriate materials they should report this to an adult immediately and take appropriate action to hide the screen or close the window, so that an adult can take the appropriate action.

Learners/Pupils should be taught and encouraged to consider the implications for misusing the internet and posting inappropriate materials to websites, for example, as this may have legal implications.

Responding to incidents of misuse:

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities.

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

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by other people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below).
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
    - Internal response or discipline procedures.
    - Involvement by Local Authority or national/local organisation (as relevant).
    - Police involvement and/or action.
    - If content being reviewed includes images of child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the Police would include:
        - Incidents of ‘grooming’ behaviour.
        - The sending of obscene materials to a child.
        - Adult material which potentially breaches the Obscene Publications Act.

- Criminally racist material.
- Other criminal conduct, activity or materials.
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the college/school and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

APPENDIX 1

Secure transfer of data and access off site

Ambitious about Autism recognises that personal data may be accessed by users off site, or transferred to the LA or other agencies. In these circumstances:

- Users may not remove or copy sensitive or restricted or protected personal data from AAA or authorised premises without permission and unless the media is encrypted and password protected and is transported securely for storage in a secure location
- Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (e.g. family members) when out of premises.
- When restricted or protected personal data is required by an authorised user from outside the organisation’s premises (for example, by a member of staff to work from their home), they should preferably have secure remote access to the management information system or learning platform
- If secure remote access is not possible, users must only remove or copy personal or sensitive data from the organisation or authorised premises if the storage media, portable or mobile device is encrypted and is transported securely for storage in a secure location
- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software; and
- Particular care should be taken if data is taken or transferred to another country, particularly outside Europe.

APPENDIX 2

E-safety Agreement

(Staff/Volunteer)

New technologies have become integral to the lives of children and young people in today's society, both within colleges and schools and in their lives outside. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- That staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- AaA ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- That staff are protected from potential risk in their use of ICT in their everyday work.

AAA will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for learners and pupils learning and will, in return, expect staff and volunteers to agree to be responsible users.

This policy applies to any device. It applies across the whole network and includes Wi-Fi.

Your activity on the internet is closely monitored; logs are kept of activity, whether on a AAA, College or school device or using your own device through the Wi-Fi. These logs include who is accessing what material for how long from which device.

The AAA email system is provided for educational and business purposes, where required the AAA has the ability to access your email for safeguarding purposes.

Acceptable Use Policy Agreement

I understand that I must use AAA's ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that learners and pupils receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

For my professional and personal safety:

- I understand that AAA will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to AaA ICT systems (e.g. laptops, email etc.) out of AAA/college/school, and to the transfer of personal data (digital or paper based) out of college/school.
- I understand that AAA ICT systems are primarily intended for Buisiness and

educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by AAA.

- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident; I become aware of, to the appropriate person.

I will be professional in my communications and actions when using AAA ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the policy on the use of digital/video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use chat and social networking sites in accordance with the policy
- I will only communicate with learners/pupils and parents/carers using official AAA systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

AAA has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the business:

- When I use my mobile devices (PDAs/laptops/mobile phones/USB devices etc.), I will follow the rules set out in this agreement, in the same way as if I was using AAA equipment. I will also follow any additional rules about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes).
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to AAA equipment, or the equipment belonging

to others.

- I will only transport, hold, disclose or share personal information about myself or others as outlined in this E-Safety Policy. Where digital personal data is Transferred outside the secure local network, it must be encrypted. Paper based Protected and restricted data must be held in lockable storage.
- I understand that Data Protection Policy requires that any staff or learner/pupil data, to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for business sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work is protected by copyright; I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of AAA:

- I understand that this Acceptable Use Agreement applies not only to my work and use of AAA ICT equipment on the premises, but also applies to my use of AAA ICT systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment.
- I understand that if I fail to comply with this Acceptable Use Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and in the event of illegal activities the involvement of the police.

Ambitious
about Autism

E-Safety Agreement (Staff/Volunteer/Contractor/Consultant) 2017

I have read and understand the E-safety policy and agree to use the AAA ICT systems (both in and out of premises) and my own devices (on any AAA premises including the college and school and when carrying out communications related to AAA) within these guidelines.

Staff/Volunteer Name

Signed

Date

APPENDIX 3

E-Safety Agreement (Parent/Carer) 2017

Digital technologies have become integral to the lives of children and young people, both within colleges and schools and outside. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Children and Young adults should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- That parents/carers will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- That AAA systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

AAA will try to ensure that learners/pupils will have good access to digital technologies to enhance their learning and will, in return, expect the learners/pupils to agree to be responsible users.

This policy applies to any device in college/school. It applies across the whole network and includes Wi-Fi.

AAA carries out secure content inspection (SSL inspection). This means that when you access a site that uses techniques to secure the information between the website and yourself, AAA can read the information and remove inappropriate content or prevent access to the material. Excluded from this inspection are sites that contain sensitive financial information, including banks and payment systems.

Your activity on the internet is closely monitored by AAA; logs are kept of activity, whether on a college/school device or using your own device through the Wi-Fi. These logs include who is accessing what material for how long from which device.

The AAA email system is provided for educational and business purposes, where required AAA has the ability to access email, for safeguarding purposes and should a management requirement necessitate it.

Acceptable Use Policy Agreement

I understand that I must use AAA ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

For my own personal safety:

- I understand that AAA will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc.)
- I will immediately report any unpleasant or inappropriate material or messages

or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

- I understand AAA systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use AaA systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube), unless I have permission of a member of staff to do so.

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I recognise that AAA has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of AAA:

- I will only use my own personal devices (mobile phones/USB devices etc.) if I have permission. I understand that, if I do use my own devices, I will follow the rules set out in this agreement, in the same way as if I was using AAA equipment.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person/organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will not install or attempt to install or store programmes of any type on any AAA device, nor will I try to alter computer settings.
- I will only use social media sites with permission and at the times that are allowed.

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of AAA premises:

- I understand that AaA also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of college or school and where they involve my membership of the college or school community (examples would be cyber-bullying, use of images or personal information).

- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to local or legal action.

Please complete the sections on the next page to show that you have read, understood and agree to this policy. If you do not sign and return this agreement, access will not be granted to AAA systems and devices.

Ambitious about Autism

Ambitious about Autism
E-safety Agreement
(Parent/Carer) 2017

This form relates to the e-safety policy, to which it is attached.

Please complete the sections below to show that you have read, understood and agree to the rules included in this policy. If you do not sign and return this agreement, access will not be granted to AAA ICT systems.

I have read and understand the above and agree to follow these guidelines when:

- I use AaA systems and devices (both in and out of their premises)
- I use my own devices in AAA sites (when allowed) e.g. mobile phones, gaming devices USB devices, cameras etc.
- I use my own equipment out of AAA sites in a way that is related to me being a member of this college/school e.g. communicating with other members of the college/school, accessing college/school email, website etc.

Name of Parent/Carer (PRINT)	
Signed by Parent/Carer	
Date	