Ambitious about Autism
E-safety Policy

November2021

This policy refers to 'the organisation' throughout and in doing so is referring to both Ambitious about Autism (AaA) and Ambitious about Autism Schools Trust (AaAST)

Contents

Policy Owner	Deputy CEO	Review Date:	December 2022
Policy No.	068	Version No.	1.0

1. Scope of the Policy

E-safety can be very broadly defined as the safe use of technology. Technology is a very broad term. More specifically, e-safety can also be called 'internet safety', 'online safety' or 'web safety'. This includes the use of the internet and also other means of communication or accessing data or information using electronic media (e.g. text messages, gaming devices, email etc).

In practice, e-safety is as much about behaviour as it is electronic security. E-safety in this context is classified into three areas of risk:

- Content: being exposed to illegal, inappropriate, or harmful material
- Contact: being subjected to harmful online interaction with other users
- Conduct: personal online behaviour that increases the likelihood of, or causes, harm.

This e-Safety policy recognises the commitment of the organisation to e-Safety for all the organisation's pupils, students and people and acknowledges its part in overall safeguarding policies and procedures. We believe the whole organisation 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, supported by the proper, appropriate, and managed use of technology that will enable us to reduce the risks whilst continuing to benefit from the opportunities.

This policy explains how the organisation's ICT resources are to be used and what actions are and are not allowed. Whilst 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 Head of IT or any member of the Senior Leadership Team (SLT) or the Executive Leadership Team (ELT).

Other policies to be referred to:
- ICT Acceptable Usage Policy
- Data Security Policy
- Data Protection Policy
- Confidentiality Policy
- Disciplinary Policy
- Grievance Policy
- Child Safeguarding and Protection Policy
- Adult Safeguarding and Protection Policy
- 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:
- Data Protection Act 2018 and the associated General Data Protection Regulations (GDPR) that this enacts;
- Computer Misuse and Cybercrimes Act;
- Regulations of Investigatory Powers Act;
- Obscene Publications Act;
- Copyright, Design and Patents Act;
- Communications Act;
- Digital Economy Act.

2. Policy Review

The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technology, new threats to e-safety or incidents that have taken place, or a significant change in government guidance or legislation affecting this policy.

The next anticipated review date will be October 2022.

Policy Owner	Deputy CEO	Review Date:	December 2022
Policy No.	068	Version No.	1.0

Page 3 of 13

3. Roles and Responsibilities

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

Finance and Resourcing Committee

The AaA/AaAST Finance and Resourcing Committee are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy.

The Executive Principal, Head of College, Heads of School and Managers

- have a duty of care for ensuring the safety (including e-safety) of members of the college and school community. This responsibility is additionally delegated to all teaching and support staff involved with any teaching and learning involving the use of IT within and school or college setting.
- be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff;
- ensure that relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant;
- ensure that there is a system in place to allow for monitoring and support of those in the organisation 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.

Designated Safeguarding Leads

Designated Safeguarding Leads (DSLs) should be trained in e-safety issues and be aware of the potential for serious safeguarding issues to arise from:

- sharing of personal or private data;
- access to, viewing of or sharing illegal/inappropriate material;
- inappropriate online contact with adults/strangers;
- potential or actual incidents of grooming;
- cyber-bullying;
- scams.

Head of IT

- Create and maintain the organisation's E-safety policy;
- Refer all e-safety incidents to the relevant safeguarding lead and assisting them as required;
- Receive reports of e-safety incidents and assist, signpost or refer as appropriate;
- Ensure the organisation's technical infrastructure is secure and is not open to misuse or malicious attack;
- Ensure that users may only access networks, resources, and devices through an enforced password protection system;
- Ensure the use of multi-factor authentication when accessing the organisation's systems or devices remotely;
- 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;
- Monitor the use of the network, internet, email, and software solutions in order that any misuse or attempted misuse can be reported to the relevant safeguarding lead;

- Ensure that monitoring software/systems are appropriately implemented and updated regularly.

All Staff

- Ensure they have read the organisation's E-Safety Policy;
- They have read, understood, and signed the ICT Acceptable Usage Policy (Staff and Volunteers);
- They report any suspected misuse or problem to the Executive Principal, Head of College, Head of School, SMY or ELT Member or the Head of IT.
- Ensure learners and pupils understand and follow the e-safety and Acceptable Usage Agreements;
- Monitor the use of devices and digital technology at work, in lessons and other activities through the use of appropriate firewall and software solutions and implement current policies with regard to these devices;
- In lessons where internet use is pre-planned, learners and pupils should be guided to websites or other networked on online resources checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Parents and Carers

Parents and Carers play a crucial role in ensuring that their children or young adults in their care understand the need to use the internet and computer or mobile devices in an appropriate way. The schools and college 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 schools/ college in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school and college events;
- children and young peoples' personal or mobile devices in the school and college (where this is allowed).

4. Policy Statements

Pupils and Learners

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils and learners to take a responsible approach. The education of pupils and learners 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 and online risks and build their online resilience.

E-Safety should be a focus in all areas of the curriculum as appropriate, 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 part of the first week of study and regularly revisited;
- Key e-safety messages should be repeatedly reinforced as part of a planned programme of training activities;
- Pupils/Learners should be taught to be aware of the materials / content they access on-line and be guided to question and validate the accuracy of information;
- Pupils/Learners should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet;
- Pupils/Learners should be helped to understand and be encouraged to adopt safe and responsible use of the internet and social media both within and outside the school and college;
- 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 pupils/learners be guided to websites or online resources which have been pre-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 pupils/learners 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 and shared with the Head of IT for review.

Parents and Carers

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

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

- Curriculum activities;
- Letters, newsletters, organisational website;
- Parents/Carers evenings/sessions;
- High profile events/campaigns e.g. Safer Internet Day.

Policy Owner	Deputy CEO	Review Date:	December 2022
Policy No.	068	Version No.	1.0

Staff and Volunteers

- As part of their induction, all new staff and volunteers should familiarise themselves with the organisation's E-safety policy and review and complete the ICT Acceptable Usage Agreement;
- This E-safety policy and its updates should be presented and discussed by staff in staff team meetings/INSET days, organisation meetings;
- A planned programme of formal e-safety training should be made available to staff as required.

IT infrastructure, Access, and Monitoring

The organisation is responsible for ensuring that the infrastructure and network is as safe and secure. In order to achieve this:

- There will be regular reviews and audits of the safety and security of technical systems;
- There will be web filtering, and reporting of inappropriate activity of users on the organisation's systems and users are made aware of this in the ICT Acceptable Use Policy. (Sophos)
- There will be web and keystroke monitoring on pupil/learner activity and reporting of inappropriate activity of pupils/learners on the organisation's systems and allocated devices. (Smoothwall)
- All users will have clearly defined access rights to 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;
- All users will use Multi-factor authentication as and when the organisation deems it necessary when accessing its systems remotely;
- The provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors, consultants, and contractors) onto the organisation's system will be managed per procedures developed by the Head of IT.

Mobile Phones and Portable Devices Provided by the Organisation

The organisation issues mobile phones and tablets to some of its employees based on job requirements. Where such a device has been issued, it is primarily for business use and at all times will remain the property of the organisation. The user will be responsible for its safekeeping, appropriate use, condition, and eventual return to the organisation.

If a device is lost or stolen this should be reported to the Head of IT.

Bring Your Own Device (BYOD) – Staff and Volunteers

Staff and volunteers may bring their own personal, electronic devices into work settings. These may include mobile phones, laptops, or tablets. The organisation provides internet access only for BYOD's through its wireless networks at no cost to staff, access to the organisations local area network, including network drives and local applications, is not allowed.

When accessing the network or using a personal mobile electronic device within the organisation's settings, staff and volunteers must abide by this E-Safety Policy, as well as the IT Acceptable Usage Policy.

When working on work-related documents, staff should be signed into their work account, as they would be, were they working on an organisational device. Work-related activity should be completed on an organisational device when possible.

Staff and volunteers bring their devices to the organisation's premises at their own risk and IT staff are under no obligation to provide any technical support beyond basic support to connect with the organisation's networks on either hardware or software. Furthermore, the safe and secure storage of that device whilst not in use is entirely the responsibility of the member of staff to whom the device belongs.

The use of a personal mobile or electronic device by staff is strictly not allowed in classrooms or teaching environments, or at any point when working with pupils or learners. Staff and volunteers should only use any personal mobile or electronic device in specifically designated areas within each setting. Staff who work with pupils or learners using any device as part of their learning or as part of the curriculum should be doing so on an organisational device. Work of this nature must never be done on a staff member's personal device.

If, as part of their work, staff communicate with pupils or learners by text, email or phone, this must be done using a work-issued device. Staff should not communicate with pupils or learners using a personal device.

Bring Your Own Device – Pupils and Learners

Pupils and Learners may bring their own personal mobile electronic devices to school/college (phones, tablets etc.) at the discretion of SLT. The organisation can provide internet access only through its wireless networks at no cost to pupils or learners, access to the organisations local area network, including network drives and local applications, is not allowed. Pupils and learners can access the networks or use a personal mobile electronic device in school or college if their parent or carer has completed an ICT Acceptable Use Form (Pupils and Learners).

The use of a personal mobile electronic device may not be appropriate in all learning environments. Pupils and learners, supported by staff, should follow the local procedure in place in each particular educational setting with regard to when the use of a personal mobile electronic device is acceptable.

Data Protection

An essential e-safety consideration is that everyone covered by this policy should have a working awareness of GDPR. GDPR stands for General Data Protection Regulations. This is to prevent a data breach or any processing of personal data that is not compliant with the law. Learners and students should be supported to understand their rights under GDPR as part of the organisation's e-safety provision.

For most staff there will be a knowledge of GDPR separate from, and parallel to, e-safety based upon their training around the processing of personal data in their role. They will be aware of the lawful basis under which they access, process or share data (which will be included in process documentation) - whether it be contractual, legitimate interest or consent - and understand what a data breach is and recognise a subject access request.

Using Digital and Video Images

Making and using digital and video images can provide benefits in a learning environment and for the organisation. However, staff, parents and carers, pupils and learners need to be aware of the risks associated with publishing digital images on the internet, or social media platforms. Such images may provide avenues for cyberbullying to take place or attract other undesirable or inappropriate attention. Such images. may in some instances provide detail or information which

Policy Owner	Deputy CEO	Review Date:	December 2022
Policy No.	068	Version No.	1.0

Page 8 of 13

could be used to identify a young person's whereabouts, and all staff and parents should be aware of this risk. Digital images may remain available on the internet indefinitely and may cause harm or embarrassment to individuals in the short or longer term.

When using or working with (making) digital images or video, staff should inform and educate pupils and learners about the risks associated with the taking, use of, sharing, publication and distribution of digital content or material. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social media platforms.

Parents and carers are welcome to take videos and digital images of their child or young adult at school or college events for their own personal use but should not video other children. In order to respect the privacy of pupils & learners, these images should not be published or made publicly available on social media platforms nor should parents and carers comment on any activities involving other learners or pupils in the digital or video images.

Staff and volunteers are allowed to take digital and video images to support educational aims, but must follow the organisation's policy concerning the sharing, distribution, and publication of those images. Images should only be taken on the organisation's equipment.

Care should be taken when taking digital or video images that pupils and learners are appropriately dressed and are not participating in activities that might bring the individuals or the organisation into disrepute or lead to any breach of our Code of Conduct or Safeguarding Policies.

Pupils and learners must not take, use, share, publish or distribute images of others without their permission.

Written permission from individuals, or where appropriate their parents or carers, will be obtained before photographs, video or other media are published.

Pupils' and learners' work can only be published with the permission of the pupil or learner and parents or carers.

Use of Social Media

Staff and volunteers should refer to the organisations Social Media Policy.

Prevent Duty

The organisation is committed to providing a safe and secure environment for children and young people where they feel safe and are kept safe. The Preventing Extremism and Radicalisation Policy is one element within our overall organisation's arrangements to safeguard and promote the welfare of all children and adults. Staff and volunteers should refer to the Preventing Extremism and Radicalisation Policy and act accordingly if they have any concerns that a pupil, learner, staff member of volunteer is at risk of extremism or radicalisation as a result of their use of the internet or social media.

Appropriate and Inappropriate Use – Staff and Volunteers

Staff members have access to the network to conduct their work and in an educational setting 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 ICT Acceptable Usage Policy, which they need to sign and return, to keep under file with a signed copy returned to the member of staff. When accessing any Learning Platform in use by AaA/AaAST from home, the same ICT Acceptable Usage Policy will apply.

If a member of staff is believed to misuse the internet or learning platform in an inappropriate, abusive, or illegal manner, a report must be made to the Designated Safeguarding Lead immediately and then the Safeguarding Policy must be followed.

Policy Owner	Deputy CEO	Review Date:	December 2022
Policy No.	068	Version No.	1.0

Appropriate and Inappropriate Use - Pupils and Learners

Pupils and learners have access to the network to support their education. Digital technologies have become and are now integral to the lives of children and young people, both within school and college and more generally. These technologies are powerful tools which should be used in a safe and appropriate way. The organisation should encourage parents and carers to support the agreement with their child or young adult. This can be shown by signing the ICT Acceptable Usage Agreement (Pupils and Learners).

As an organisation, we also engage with a number of other autistic children and young people. We have developed rules of engagement, for example through our online peer support work, and these rules, content agreements and approved principles of conduct must be adhered to, as part of keeping children and young people with whom we engage safe.

If a member of staff believes that a pupil or learner has misused the internet, social media platform or learning platform in an inappropriate, abusive or illegal manner, or has as a result of their use has undertaken or is likely to undertake an activity that will lead them to suffer or be likely to suffer significant harm then a report must be made to the Designated Safeguarding Lead immediately and then the Safeguarding Policy must be followed.

5. Key Additional Resources

Key Resources

GOV.UK Safeguarding in Schools, Colleges & Other Providers
https://www.gov.uk/government/publications/covid-19-safeguarding-in-schools-colleges-and-other-providers/coronavirus-covid-19-safeguarding-in-schools-colleges-and-other-providers

GOV.UK Safeguarding & Remote Education during C19
https://www.gov.uk/guidance/safeguarding-and-remote-education-during-coronavirus-covid-19

LGfL Online Safeguarding Guidance
https://coronavirus.lgfl.net/safeguarding

NCSC – VC Services Security Guidance
https://www.ncsc.gov.uk/guidance/video-conferencing-services-security-guidance-organisations

SWGfL
https://swgfl.org.uk/

6. Additional Resources (COVD-19 focussed) (2020/21)

The guidance below is based on the LGfL C19 Closure Safe Policy Updates. The guidance below *does not form part of this formal policy* but is intended to support the spirit and intent of the policy and provide additional, reliable resources for school, colleges, parents, and carers specifically during the C19 pandemic. This section will be reviewed (and possibly removed) in the October 2021 review of this policy.

Online safety in schools and colleges

As more children return to education settings, it will be important that schools and colleges continue to provide a safe online environment for those who remain at home. Schools and colleges should continue to ensure that appropriate filters and monitoring systems are in place to protect children when they are online on the school or college's IT systems.

- The UK Council for Internet Safety provides information to help governing bodies and proprietors assure themselves that any new arrangements continue to effectively safeguard children online.

- Internet Matters vulnerable children in a digital world-report may help governing bodies, proprietors, senior leaders and DSLs understand more about the potential increased risks some groups of children can face online.

- The NSPCC Learning website also provides useful support and training opportunities for professionals.

Children and online safety away from school and college

All schools and colleges should be doing what they reasonably can to keep all their children safe. Whilst more children return to school and college, others will continue to stay at home and, in many cases, will be continuing to engage with their school or college online.

It is important that all staff who interact with children, including online, continue to look out for signs a child may be at risk. Any such concerns should be dealt with as per the child protection policy and where appropriate referrals should continue to be made to children's social care and as required the police.

Remote education

The department has provided guidance on safeguarding and remote education to support schools and colleges plan lessons safely. Case studies are available for schools to learn from each other's emerging practice as they develop their approaches to providing remote education.

Virtual lessons and live streaming

There is no expectation that teachers should live stream or provide pre-recorded videos. Schools and colleges should consider the approaches that best suit the needs of their children and staff. Guidance from the National Cyber Security Centre on which video conference service is right for you and using video conferencing services securely can help set up video conferencing safely, if you choose to use it.

In addition, guidance from the UK Safer Internet Centre on safe remote learning includes detailed advice for real time online teaching and the London Grid for Learning safeguarding advice includes platform specific advice.

Policy Owner	Deputy CEO	Review Date:	December 2022
Policy No.	068	Version No.	1.0

Page 11 of 13

Teaching from home is different to teaching in the classroom. Teachers should try to find a quiet or private room or area to talk to pupils, parents, or carers. When broadcasting a lesson or making a recording, also consider what will be in the background.

Online safety

All schools and colleges should continue to consider the safety of their children when they are asked to work online. The starting point for online teaching should be that the same principles as set out in the school's or college's staff behaviour policy (sometimes known as a code of conduct) should be followed. This policy should amongst other things include acceptable use of technologies, staff pupil/student relationships and communication including the use of social media. The policy should apply equally to any existing or new online and distance learning arrangements which are introduced.

Schools and colleges should, as much as is reasonably possible, consider if their existing policies adequately reflect that some children (and in some cases staff) continue to work remotely online. As with the child protection policy, in some cases an annex/addendum summarising key coronavirus related changes may be more effective than re-writing/re-issuing the whole policy.

The principles set out in the guidance for safer working practice for those working with children and young people in education settings published by the Safer Recruitment Consortium may help schools and colleges satisfy themselves that their staff behaviour policies are robust and effective. In some areas schools and colleges may be able to seek support from their local authority when planning online lessons/activities and considering online safety.

Schools and colleges should continue to ensure any use of online learning tools and systems is in line with privacy and data protection requirements.
An essential part of the online planning process will be ensuring children who are being asked to work online have very clear reporting routes in place so they can raise any concerns whilst online. As well as reporting routes back to the school or college this should also signpost children to age appropriate practical support from the likes of:

- Childline - for support
- UK Safer Internet Centre - to report and remove harmful online content
- CEOP - for advice on making a report about online abuse

Schools and colleges are likely to be in regular contact with parents and carers. Those communications should continue to be used to reinforce the importance of children being safe online. It will be especially important for parents and carers to be aware of what their children are being asked to do online, including the sites they will asked to access and be clear who from the school or college (if anyone) their child is going to be interacting with online.

Parents and carers may choose to supplement the school or college online offer with support from online companies and in some cases individual tutors. In their communications with parents and carers, schools and colleges should emphasise the importance of securing online support from a reputable organisation/individual who can provide evidence that they are safe and can be trusted to have access to children.

Policy Owner	Deputy CEO	Review Date:	December 2022
Policy No.	068	Version No.	1.0

Support for parents and carers to keep their children safe online includes:

- [Thinkuknow](#) provides advice from the National Crime Agency (NCA) on staying safe online
- [Parent info](#) is a collaboration between Parentzone and the NCA providing support and guidance for parents from leading experts and organisations
- [Childnet](#) offers a toolkit to support parents and carers of children of any age to start discussions about their online life, to set boundaries around online behaviour and technology use, and to find out where to get more help and support
- [Internet Matters](#) provides age-specific online safety checklists, guides on how to set parental controls on a range of devices, and a host of practical tips to help children get the most out of their digital world
- [London Grid for Learning](#) has support for parents and carers to keep their children safe online, including tips to keep primary aged children safe online
- [Net-aware](#) has support for parents and carers from the NSPCC and O2, including a guide to social networks, apps, and games
- [Let's Talk About It](#) has advice for parents and carers to keep children safe from online radicalisation

Government has also provided:
- [support for parents and carers to keep children safe from online harms](#), includes advice about specific harms such as online child sexual abuse, sexting, and cyberbullying
- [support to stay safe online](#) includes security and privacy settings, blocking unsuitable content, and parental controls

The department encourages schools and colleges to share this support with parents and carers.