# Ambitious about Autism
# E-safety Policy

# November 2019

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



| | | | |
|---|---|---|---|
| Policy Owner | Head of Property and IT | Review Date: | November 2020 |
| Policy No. | 068 | Version No. | 2.1 |

# 1. Scope of the Policy

This e-Safety policy recognises the commitment of the organisation to e-Safety for all the organisation's pupils, students and staff 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 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 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:

- 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 technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be November 2020.

# 3. Roles and Responsibilities

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

## Scrutiny and Audit Committee and Finance and Resourcing Committee

The Scrutiny and Audit Committee of Ambitious about Autism and the Finance and Resourcing Committee of the Ambitious about Autism Schools Trust are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy.

I should be noted that 14 November 2019 is that last time these two groups will meet separately. Future meetings will be joint, and the new joint group will carry approval responsibility for this e-safety policy.

## The Executive Principal, Principal, Headteachers and Managers

- have 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 may be delegated to an E-Safety Co-coordinator at a particular school or college site;
- 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 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 illegal/inappropriate materials;
- inappropriate online contact with adults/strangers;
- potential or actual incidents of grooming;
- cyber-bullying.

## Head of Property & 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 create a log of incidents;
- Ensure the organisation's technical infrastructure is secure and is not open to misuse or malicious attack;
- Ensure that users may only access networks and devices through an enforced password protection system;
- Ensure the use of multi-factor authentication when accessing the organisation's systems 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 and email in order that any misuse or attempted misuse can be reported to the relevant safeguarding lead;
- Ensure that monitoring software/systems are 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, Principal, relevant Head Teacher ELT Member or Head of IT;
- Ensure learners and pupils understand and follow the e-safety and acceptable use 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 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.

## 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 mobile devices in an appropriate way. The college and schools 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 and college events;
- children and young peoples' personal 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 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 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 reinforced as part of a planned programme of training activities;
- Learners/Pupils should be taught to be 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 of the internet and social media 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 and shared with a senior member of staff 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.

## 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, monitoring 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.
- 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 mobile electronic devices to work (phones, tablets etc.). The organisation provides internet access through its wireless networks at no cost. When accessing the network or using a personal mobile electronic device on the organisations premises, staff and volunteers must abide by this E-Safety Policy.

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.

The use of a personal mobile electronic device may not be appropriate in all learning environments. Staff and volunteers should follow the local procedures in place in each particular educational setting

with regard to when the use of a personal mobile electronic device is acceptable. There are some learning environments where having a personal or work device about one's person is not permitted in the interests of pupil or learner safety.

## Bring Your Own Device – Pupils and Learners

Pupils and Learners may bring their own personal mobile electronic devices to school/college (phones, tablets etc.). The organisation provides internet access through its wireless networks at no cost. Pupils and learners can access the network or using 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. 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. 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 digital images or video, staff should inform and educate pupils and learners about the risks associated with the taking, use, 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. 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 parents or carers will be obtained before photographs of pupils and learners are published on the organisation's websites.

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 secure environment for children and young people where they feel safe and are kept safe. This 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 the Learning Platform 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.

## 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)

If a member of staff believes that a pupil or learner has misused the internet 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.

**END**

**Version Control**

| | |
|---|---|
| Version | 2.1 |
| Last edited by | Mark Dixon<br>(Head of Property & IT) |
| Date of last edit | 24 October 2019 |
| Hyperlinks checked | 24 October 2019 |
| Review Date | November 2020 |