BeyondAutism
Schools

E-SAFETY POLICY

Registered Charity in England and Wales No. 1082599. Registered Company No. 4041459.
Registered Office: Ashurst LLP, London Fruit & Wool Exchange, 1 Duval Square, London, E1 6PW

E-Safety and Acceptable Usage

Introduction

New technologies have revolutionised the movement, access and storage of information with important implications for all schools. Use of ever more powerful computers, broadcast media, the Internet, digital recorders of sound and images together with increased opportunities to collaborate and communicate are changing established ideas of when and where learning takes place. At BeyondAutism Schools, we recognise that learning is a lifelong process and that e-learning is an integral part of it. Ensuring that we provide pupils with the skills to make the most of information and communication technologies is an essential part of our curriculum. The school is committed to the continuing development of our ICT infrastructure and embracing new technologies so as to maximise the opportunities for all pupils, staff, parents and the wider community to engage in productive, cooperative and efficient communication and information sharing.

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

- Access to illegal, harmful or inappropriate images or other content.
- Un-authorised access to / loss of / sharing of personal information.
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge.
- Inappropriate communication / contact with others, including strangers.
- Cyber-bullying.
- Access to unsuitable video / internet games.
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is used in conjunction with other school policies (e.g. behaviour, anti-bullying and safeguarding policies).

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

This policy sets out clearly our expectations on pupils, staff, parents and members of the wider community to ensure best practice.

Scope of the Policy

This policy applies to all members of the school community (including staff, governors, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

Roles and Responsibilities

Governors

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy.

Heads of School / Senior Leaders

- The Heads of School are responsible for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the Head of Pastoral.
- The Heads of School are responsible for the implementation and effectiveness of this policy. They are also responsible for reporting to the Governing Body on the effectiveness of the policy and, if necessary, make any necessary recommendations re further improvement.
- The Heads of School / Senior Leaders are responsible for ensuring that the Head of Pastoral and other relevant staff receive suitable Continuous Professional Development to enable them to carry out their e-safety roles.
- The Heads of School / Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school 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.
- The Heads of School and another member of the Senior Leadership Team 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. (See Safeguarding - Managing Allegations against a member of staff policy/guidance).

Heads of Pastoral

- Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school 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.
- Reports to the School Leadership Team and BeyondAutism's Senior Management Team serious breaches of the E-Safety Policies.
- Provides training and advice for staff.
- Liaises with the Local Authority.
- Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments.

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 school e-safety policy and practices.
- They have read, understood and signed the E–Safety policy.
- They report any suspected misuse or problem to the Head of Pastoral for investigation / action / sanction.
- Digital communications with pupils and parents / carers (email / voice) should be on a professional level.
- Pupils understand and follow, as appropriate for age and ability, the school e-safety and acceptable use policy.
- Pupils understand and follow E-Safety rules to the best of their ability and they know that if these are not adhered to, sanctions may be implemented in line with our behaviour and anti-bullying policies.
- In lessons where internet use is planned 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.

Designated Safeguarding Lead/Head of Pastoral

Should be trained in e-safety issues and be aware of the potential for serious child protection 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.
- Sexting.
- Revenge pornography.
- Radicalisation (extreme views).
- Child Sexual Exploitation.

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and may be less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through parents' evenings, letters, website / local e-safety campaigns / literature.

Parents / carers should understand that school has a duty of care to all pupils. The misuse of non-school provided systems, out of hours, will be investigated by the school in line with our behaviour, anti-bullying and safeguarding policies.

Pupils

We expect pupils to save and keep their work to build up a portfolio of evidence. Pupils are taught how to save their work into their “My documents” area.

We expect pupils to respect the privacy of all other users and to make no attempt to access or interfere with another user’s work. Pupils will be taught not to access another user’s work without permission

We expect pupils to respect the contributions of others, not to delete or alter others’ work and to ensure that they only save work to shared areas with permission. Pupils will be taught how to access and save to these shared resource areas.

We expect pupils to only print out work when directed by staff to do so.

We expect all users to make no attempt to load or download any programme onto the network.

Pupils will be taught that their use of the network can be monitored.

Internet Safety

BeyondAutism will be responsible for ensuring that the school 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:

- School ICT systems will be managed through the managed service provider, in ways that ensure that the school meets the e-safety technical requirements.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to school ICT systems.
- Staff will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- BeyondAutism maintains and supports the managed filtering service. Any incidents or activities regarding filtering will be reported in accordance with this policy.
- Remote management tools are used by the managed service provider to control workstations and view users’ activity.
- Appropriate security measures are in place, provided by the managed service provider, to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data.
- Guest access to the school network will be authorised by the Heads of School through the provision of limited access guest accounts which do not give access to personal information about pupils or staff.

- The school infrastructure and individual workstations are protected by up to date anti-virus software.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured in accordance with the IT and Computer Use Policy.

Content filtering

BeyondAutism will use *Cisco Meraki* content filtering for devices managed by the organisation and devices using company internet/Wi-Fi. This allows certain categories of websites to be blocked based on certain criteria, in addition to specific named websites. More information can be found at: https://documentation.meraki.com/MX/Content_Filtering_and_Threat_Protection/Content_Filtering

Email Safety

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

- The official school email service may be regarded as safe and secure. Pupils should therefore not use other email systems when in school, or on school systems.
- Users need to be aware that email communications may be monitored.
- Users must immediately report, to the Head of Pastoral – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and pupils or parents / carers must be professional in tone and content and be via official used systems.
- Whole class or group email addresses may be provided to all classes for educational use. Individual email addresses will be provided to some pupils if deemed appropriate for their level of ability by their class supervisor.
- Pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be placed on the school website on public facing calendars and only official school emails should be identified within it.
- BeyondAutism allows staff to bring in their own personal devices, including mobile phones, for their own use in accordance with the Bring Your Own Device Policy. Under no circumstances should a member of staff use their personal devices including mobile phones, to contact a pupil, parent/carer. Further information on this can be found in the Code of Conduct.

Curriculum

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT across the curriculum.

- Good E-Safety practice is an integral part of the school PSHE curriculum and will be taught to pupils as part of their NET learning and development of communication skills.
- Pupils that have computing lessons will also focus on E-safety for half a term as part of the computing curriculum.
- Where pupils are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.

Digital Images

- Digital still and video cameras are used for recording special events as well as being essential tools for everyday learning experiences across the curriculum. As part of pupil induction, parents are asked to sign a consent form for images of their children to be used for school and/or charity purposes. Some images celebrating the work of pupils involved in everyday and special event activities may be selected to be shown on the school website. On the website we never state a child's full name with their image. The school will happily remove any image of a child/young person on the school website at their parent's request.
- Digital images may be shared with partner schools and organisations as part of collaborative learning projects. This can include live video conferencing. All such use is monitored and supervised by staff.

Cyber-Bullying

- The school takes bullying very seriously and has robust procedures for identifying and dealing with it. Cyber-bullying is the use of any communication medium to offend, threaten, exclude or deride another person or their friends, family, gender, race, culture, ability, disability, age or religion.
- Pupils are taught about bullying as part of the PSHE curriculum. We expect all members of our community to communicate with each other with respect and courtesy. Bullying of any type will not be tolerated by the school and will be dealt with under the procedures within the Whole School Policy on Behaviour, including bullying.
- Research indicates that children with disabilities, particularly those with learning or communication difficulties, are at increased risk of cyber-bullying outside of school. This may be from people known to them, by people pretending to be their friend (mate crime) or by strangers. Pupils will be taught how to seek help if they think that someone might be bullying them online, including how to capture a screen.
- Children with learning disabilities may be targeted by others for the purpose of abuse. This can take many forms including sexual exploitation, grooming for sexual abuse or mate crime – where a person pretends to be a friend or supporter in order to benefit in some way – possibly financially, materially or for entertainment. Pupils will be taught that friends are people who do not hurt us or ask us to do things that we don't want to do and that they should not have friends on the internet that they do not know in real life.

Mobile Phones

- Pupils are not permitted to have mobile phones upon their person in school unless it is part of an agreed programme or IEP goal monitored by staff.

- If it is believed that a pupil does have a mobile phone in school, we will ask the pupil to hand the phone to a member of staff. If the pupil cannot be persuaded to hand in the phone, staff will if necessary, search the child and / or their bag in line with national guidance (schools' powers to search) and the BeyondAutism policy for physical intervention.
- Staff must not:
  - Have their mobile phones with them during teaching time.
  - Use their mobile phones to take photos/film of the children.
  - Allow the children to play games/music on their mobile phones.
- Phones are not to be used in School/College, with the exception of pupils where it features in their Individual Program.

Please also refer to 'Parent Training' and 'Cyber Bullying'.

Other technologies

- iPads – these will be covered by the same rules as computers. Please refer to the IT and Computer Use Policy.

Copyright

- Though there are lots of free to use resources on the Internet, the majority of images, sound and music files are covered by copyright laws. Some can be used for educational reasons without permission provided that the source is stated and that they are not made available outside the school. Some cannot be used under any circumstances, this is particularly so for music but can apply to other types of file e.g. photographic images. Care therefore needs to be taken with multi-media work which incorporates anything downloaded from the Internet or any other published source that it is not uploaded onto the school's website or broadcast through any other technology.
  We expect all users to respect copyright laws.

Data Protection Act 1998

- The Data Protection Act 1998 gives you the right to access information held about you or your child by the school. The school has the right to charge for supplying this information. Further information on the Data Protection Act can be obtained from the Ministry of Justice – www.gov.uk/moj.

- Personal data about students will be recorded and processed in order for us to be able to offer an appropriate service to them, and to be able to collect evidence of their progress within their School life. We will also collect any data that students would like to keep, such as photos, that record their own personal achievements.

- 15.2 The way in which we collect, and process data is in line with the General Data Protection Regulation that was introduced in May 2018. More information about how we do

this can be found in our Data Protection Policy and Privacy Policy – both of which can be found on the BeyondAutism website www.beyondautism.org.uk

Training

Parents and Carers

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

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

- Letters, web site.
- Parents evenings.
- Reference to external E-Safety websites.
- High profile events such as Internet safety day.
- Family learning opportunities.

Staff

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. 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 and agree to adhere to the school e-safety policy and Acceptable Use Policies.
- The Head of Pastoral will provide advice / guidance / training to individuals as required.

Responding to Incidents of Misuse

There may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If any apparent or actual misuse by pupils, staff or any other user appears to involve illegal activity i.e.

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

The incident will be recorded in accordance with the safeguarding policy and if necessary, the police will also be informed.

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with by filling in a cause for concern form and following that procedure.

Related policies

Safeguarding, Behaviour, Anti-Bullying, IT and Computer Use, Data Protection, Code of Conduct

Last reviewed: November 2020
Date of next review: November 2023
Review Group: Executive Head

Appendices

Guidelines for the use of communication technologies within school

	Staff & other adults				Pupils			
Communication Technologies	**Allowed**	**Allowed in designated areas**	**Allowed for selected staff**	**Not allowed**	**Allowed**	**Allowed at certain times**	**Allowed with staff permission**	**Not allowed**
Mobile phones may be brought to school	x							x
Use of mobile phones in lessons				x				x
Use of mobile phones in social times		x						x
Taking photos on mobile phones or personal camera devices				x				x
Use of personal handheld devices (IPad)		x					x	
Use of personal email addresses in school, or on school network during own time	x						x	
Use of school email for personal emails				x			x	
Use of chat rooms, facilities				x				x
Use of instant messaging	x							x
Use of social networking sites			x					x
Use of personal blogs				x			x	
Use of educational blogs	x						x	