Online Safety Policy

Albright Education Centre

Sandwell Home and Hospital Tuition Service

Signed by Chair of Governors:	
Date ratified by Governing Body:	08.10.2025
Date of Review:	08.10.2026

Rationale

It is the duty of the service to ensure that every child and young person (CYP) in their care is safe, and the same principles should apply to the 'virtual' or digital world as would be applied to the real world. Increasingly, CYP are accessing material through the internet and games consoles which is not age appropriate. It is essential to address this and to encourage a lifestyle which incorporates a healthy balance of time spent using technology.

This policy for staff, governors, visitors and pupils, is to protect the interests and safety of the whole school community and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements. It is linked to the following school policies: Child Protection, Health and Safety and Behaviour.

Both this policy and the Acceptable Use Policies (for all staff, governors, visitors and pupils) are inclusive of both fixed and mobile internet, technologies provided by the school (such as PCs, laptops, whiteboards, tablet, voting systems, digital video and camera equipment, etc) and technologies owned by pupils or staff.

The Technologies

ICT in the 21st Century has an all-encompassing role within the lives of children and adults. New technologies are enhancing communication and the sharing of information. Current and emerging technologies used in school and, more importantly in many cases, used outside of school by children include:

- The Internet
- e-mail
- Instant messaging
- Blogs
- Social networking sites
- Chat Rooms
- Gaming Sites
- Text messaging and picture messaging
- Video calls
- Podcasting
- Online communities via games consoles
- Mobile internet devices such as Smart Phone and Tablets.

Whole school approach to the safe use of ICT

Creating a safe ICT learning environment includes three main elements in this service:

1. An effective range of technological tools which are filtered and monitored;
2. Policies and procedures, with clear roles and responsibilities;
3. A comprehensive e-Safety education programme for pupils, staff and parents.

Staff Responsibilities

E-Safety is recognised as an essential aspect of strategic leadership in this service and the Head Teacher, with the support of governors, aims to embed safe practices into the culture of the service. The Head Teacher ensures that the policy is implemented and compliance with the policy monitored. All staff are encouraged to create a talking culture in order to address any e-safety issues which may arise in classrooms on a daily basis. The responsibility for e-Safety has been designated to a member of the senior leadership team.

Our school **e-Safety Coordinator is Stephen Downey**

Our e-Safety Coordinator ensures he keeps up to date with e-Safety issues and guidance through liaison with Broadband Sandwell's e-Safety Officer and through organisations such as The Child Exploitation and Online Protection (CEOP). The school's e-Safety Coordinator ensures the Head, Senior Management and Governors are updated as necessary.

Staff awareness

- All staff receive regular information and training on e-safety issues in the form of in house training and meeting time.
- New staff receive information on the school's AUP as part of their induction.
- All staff are made aware of individual responsibilities relating to the safeguarding of children within the context of e-safety and know what to do in the event of misuse of technology by any member of the school community.
- All staff are encouraged to incorporate e-safety activities and awareness within their curriculum areas and through a culture of talking about issues as they arise.
- E-safety records of concern are completed by staff as soon as incidents occur and are reported directly to the school's designated safeguarding team.

All staff working with CYP are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following school e-Safety procedures. These behaviours are summarised in the AUPs which must be signed and returned before use of technologies in school.

Internet:

- The service will use Broadband Sandwell "filtered" Internet Service, which will minimise the chances of pupils encountering undesirable material.
- Staff, pupils and visitors have access to the internet through the school's fixed and mobile internet technology.
- Staff should email school-related information using their school account and not their personal accounts.
- Staff will preview any websites before recommending to pupils.
- Internet searches are conducted using the Safe Search homepage found at http://www.safesearchkids.com/.
- If internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher.
- If staff or pupils discover an unsuitable site, the screen must be switched off immediately and the incident reported to the e-safety coordinator(s) detailing the device and username. Agilisys can then be informed and contact to TrustNet can be instigated.
- Staff and pupils are aware that school based email and internet activity is monitored and can be explored further if required.
- Pupils using the World Wide Web are expected not to deliberately seek out offensive materials. Should any pupils encounter any such material accidentally, they are expected to report it immediately to a teacher and then Agilisys so that the Service Provider (TrustNet/Virgin Media) can block further access to the site.
- Pupils are expected not to use any rude or offensive language in their email communications and contact only people they know or those the teacher has approved.
- They are taught the rules of etiquette in email and are expected to follow them.
- No personal information such as phone numbers and addresses should be given out and no arrangements to meet someone made unless this is part of an approved school project.
- Pupils consistently choosing not to comply with these expectations will be warned, and subsequently, may be sanctioned following the school's behaviour policy.
- Pupils will be asked to sign to the Acceptable Use Agreement thus ensuring that they are aware of expectations. Copies of the agreement will also be distributed to parents to ensure that key messages are reinforced at home.

Passwords:

- Use a strong password (strong passwords are usually eight characters or more and contain upper and lower case letters, as well as numbers).
- Passwords should not be written down.
- Passwords should not be shared with other children or staff.

Mobile technology (laptops, iPads, netbooks, etc):

- Staff laptops should not be left in cars. If this is unavoidable, it should be temporarily locked out of sight in the boot.
- Staff should only use the laptop which is allocated to them.
- Mobile technology for pupil use, such as iPads and netbooks, are stored in a locked cupboard. Access is available via the school office, keyholders or Agilisys. Members of school staff (not visitors or children) should sign in/out the technologies before and after each use.
- Mobile Technology assigned to a member of staff as part of their role and responsibility must have a passcode or device lock so unauthorised people cannot access the content.
- Should personal devices be used to take pictures or videos of pupils (for example on trips) once downloaded onto the school system, all traces should be deleted off the personal device.
- When they are not using a device staff should ensure that it is locked to prevent unauthorised access.
- No personal devices belonging to staff or children are to be used during the school day. If staff bring in their own devices such as mobile phones, these are to be used during break times only and kept on silent. If pupils bring in mobile phones (for the purpose of safety if they walk to and from school alone), they should be kept switched off and handed in to the school office during the school day, and will remain the responsibility of the child in case of loss or damage. Any pupil not following these rules will be dealt with using the school's behaviour policy.

Data storage

- Staff are expected to save all data relating to their work to their Laptop if they have been assigned one or to the Google Drive Account.
- The school discourages the use of removable media however if they are used we expect the Encryption of all removable media (USB pen drives, CDs, portable drives) taken outside school or sent by post or courier.
- Staff laptops should be encrypted if any data or passwords are stored on them.
- IEPs, assessment records, pupil medical information and any other data related to pupils or staff should not be stored on personal memory sticks.
- Only take offsite information you are authorised to and only when it is necessary and required in order to fulfil your role. If you are unsure speak to a member of the Senior Management Team.

Social Networking Sites

- Use such sites with extreme caution, being aware of the nature of what you are publishing on-line in relation to your professional position. Do not publish any information online which you would not want your employer to see.
- Under no circumstances should school pupils or parents, past or present, be added as friends, unless known to you as a friend or relative prior to your appointment.
- Your role in school requires a high degree of professionalism and confidentiality.
- Any communications or content you publish that causes damage to the School, Local Authority, any of its employees or any third party's reputation may amount to misconduct or gross misconduct to which the School and Local Authority Dismissal and Disciplinary Policies apply. This could also undermine any complaints procedures.
- Where applications allow the posting of messages online, users must be mindful that the right to freedom of expression attaches only to lawful conduct.
- The Local Authority expects that users of social networking applications will always exercise the right of freedom of expression with due consideration for the rights of others and strictly in accordance with these Terms of Use.

Any communications made in a professional capacity through social media must not either knowingly or recklessly:

- place a child or young person at risk of harm;
- bring the Service into disrepute;
- breach confidentiality;
- breach copyright;
- breach data protection legislation; or do anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example by:
    - making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age;
    - using social media to bully another individual; or
    - posting images that are discriminatory or offensive or links to such content.

The Service reserves the right to monitor staff internet usage. The Service considers that valid reasons for checking internet usage include concerns that social media/internet sites have been accessed in breach of this Policy.

Digital images

- Use only digital cameras and video cameras provided by the school and under no circumstances use personal equipment such as digital cameras or camera phones to store images of children unless prior authorisation has been provided. If it is used in this way then images must be removed before leaving the school premises.
- Ensure you are aware of the children whose parents/guardians have **not** given permission for their child's image to be used in school. An up to date list is kept in the school administrative office.
- When using children's images for any school activity, they should not be identified by their name.

Members of staff who breach the acceptable use policy may face disciplinary action. A misuse or breach of this policy could also result in criminal or civil actions being brought against you.

Providing a comprehensive E-safety education to pupils and parents

- All staff working with children must share a collective responsibility to provide e-safety education to pupils and to promote e-safety in their own actions.
- Formally, an e-safety education is provided by the objectives contained in the ICT unit plans for every area of work for each year group. Even if e- safety is not relevant to the area of ICT being taught, it is important to have this as a 'constant' in the ICT curriculum.
- Informally, a talking culture is encouraged in classrooms which allows e-safety issues to be addressed as and when they arise.
- The ICT Coordinator will lead an assembly twice a year, including on Safer Internet Day, highlighting relevant e-safety issues and promoting safe use of technologies.
- eSafety themes are also woven into the fabric of the centre curriculum.
- When children use school computers, staff should make sure children are fully aware of the agreement they are making to follow the school's ICT guidelines.

Maintaining the security of the school IT Network

Agilisys maintains the security of the school network and is responsible for ensuring that virus protection is up to date at all times. However, it is also the responsibility of the IT users to uphold the security and integrity of the network Complaints procedure.

As with other areas of school, if a member of staff, a child or a parent / carer has a complaint or concern relating to e-safety then they will be considered and prompt action will be taken. Complaints should be addressed to the e-safety Coordinator in the first instance, who will undertake an immediate investigation and liaise with the leadership

team and those members directly involved. Incidents of e-safety concern will be recorded using a Notice of Concern proforma and reported to the school's designated safeguarding officer in accordance with school's child protection policy. Complaints of Cyberbullying are dealt with in accordance with our Anti-Bullying Policy.

Monitoring

The Head Teacher/Deputy Head Teacher or other authorised members of staff may inspect or monitor any ICT equipment owned or leased by the school at any time without prior notice.

Monitoring includes: intercept, access, inspect, record and disclose telephone calls, e-mails, instant messaging, internet/intranet use and any other electronic communications (data, e-mail, texts or image) involving employees without consent, to the extent permitted by law. This may be to confirm or obtain School business related information; to confirm or investigate compliance with School policies, standards and procedures, to ensure the effective operation of School ICT, for quality control or training purposes, to comply with a Subject Access Request under the Data Protection Act 1998, or to prevent or detect crime.

Monitoring and filtering is done by Agilisys Ltd as our ICT support provider.

Breaches of Policy

Any policy breaches are grounds for disciplinary action in accordance with the School Disciplinary Policy. Policy breaches may also lead to criminal or civil proceedings.

Incident Report

All security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's Designated Safeguarding Lead.