ACHIEVE BEYOND SCHOOLS

A B S

"We R.A.I.S.E. each other"

Online Safety Policy

Independent School Standards: paragraphs 7 and 34

Latest review and update	March 2026
Next external review and update	March 2027

AIM

At Achieve Beyond Schools, we recognise that pupils' use of the internet is an important part of their education but there are also risks associated with its use. We teach online safety across the curriculum and the Designated Safeguarding Leads (DSLs) take responsibility for online safety, ensuring that all colleagues understand and are aware of the filtering and monitoring systems in place. This policy uses the DfE's 'teaching online safety in school' guidance (last updated January, 2023) and the DfE's filtering and monitoring standards. It addresses how we seek to minimise these risks in schools and teach pupils how to stay safe when using the internet at home and outside of school. We also recognise that all colleagues must always be mindful of the need to follow our policy of acceptable use of our IT equipment.

MONITORING

We have a filtering system provided by Fortigate, which prevents pupils from accessing harmful and inappropriate content. We also have a pro-active monitoring system, provided by Senso, which allows us to monitor all internet use and provides information such as violations and blocks, as well as urgent notifications when a pupil attempts to access or search for harmful or inappropriate material. This is in addition to physical monitoring by teachers supervising screens of pupils and live supervision managed via a console through Senso. The software systems we use provide reports and the system is regularly reviewed to ensure we have effective monitoring strategies in place. While filters should not over block, as it may place unreasonable restrictions on what pupils can be taught, it is also fundamental to be aware of some of the potential dangers that the internet can pose, including:

- Access to illegal, harmful, or inappropriate images, video games or other content such as pornography, self-harm, extremism, misinformation, disinformation (including fake news) and conspiracy theories.
- Unauthorised access to/loss of/sharing of personal information.
- The risk of being subject to grooming.
- The sharing/distribution of personal images without an individual's consent or knowledge.
- Inappropriate communication/contact with others, including strangers.
- Sexting.
- Implications of geolocation (being able to track someone's location via a mobile phone or internet-connected computer).
- Cyber-bullying.
- Harmful online challenges and online hoaxes.
- An inability to evaluate the quality, accuracy and relevance of information on the internet.
- The potential for excessive use which may have a negative impact on the social and emotional development and learning of the young person.

Teaching pupils about the safe use of technology is embedded throughout the curriculum and is also taught at the beginning of every year as a unit block. Pupils are taught about online safety and risks as part of a whole school approach. Adults know to report and log any online safeguarding concerns via our online safeguarding portal and to the DSL.

THE INTERNET

We have a duty to provide pupils with quality internet access as part of their learning experience. Pupils will be taught what internet use is acceptable and what is not. All teachers involved with teaching and learning will prepare pupils to benefit safely from the opportunities presented and ensure that they have a growing understanding of how to manage the risks involved in online activity in the following ways:

- Discussing, reminding, or raising relevant online safety messages with pupils routinely, wherever suitable opportunities arise.
- Reminding pupils, colleagues and parents/carers about their responsibilities, which have been agreed through the User Agreement that all pupils and parents/carers have signed during their inductions.
- Adults will guide pupils to online activities that will support the learning outcomes planned for the pupils' age and maturity. Access levels will also be reviewed to reflect curriculum requirements.
- Teaching pupils as a planned element of personal, social, health, economic (PSHE), and computing education about online safety (paying active regard to KCSIE's 4Cs: **content**, **contact**, **conduct** and **commerce**), misuse of technology, the law in this area and how to correctly use modern technology for positive reasons.

FILTERING INTERNET ACCESS

- The advanced filtering and monitoring made available to us by Fortigate and Senso goes above and beyond that which is mandated in the latest 'Keeping Children Safe in Education' statutory guidance and the DfE 'Teaching online safety in school' guidance. However, it is not always possible to guarantee that access to unsuitable material will never occur
- The wireless network is secure and is password-protected, which prevents unauthorised access.
- All users will be required to enter their username and password before being able to access the network from any device.
- Colleagues have access to administer/download PCs and laptops that are part of our domain and they have LOCAL ADMIN access only.
- Teachers are encouraged to inspect websites they wish to use beforehand and will be responsible for all pupils who access the internet in their lessons.
- Additional filtering may be installed by the schools as and when required.
- All users are informed about what to do if inappropriate material is accessed or found on the computer.

MANAGING AND SAFEGUARDING COMPUTER SYSTEMS

The schools commission IT consultants whose responsibilities include ensuring the personal safety of adults and pupils in terms of our IT provision. It is also the IT consultants' role to work with leadersto ensure that the security of the schools' systems and its users are reviewed regularly. To support the maintenance of the schools' IT system:

- Workstations are secured against user mistakes and deliberate actions.
- Our servers are located securely and physical access is restricted to appropriate adults.
- The server operating system is secured and kept up to date.

- A firewall is maintained and virus and malware protection for the whole network is installed and current.
- Virus protection is installed and current on all laptops used for school activity.
- Access by wireless devices is proactively managed (pupils cannot access the school's wireless network unsupervised).
- Portable media may not be used without specific permission followed by a virus check.
- Unapproved software is not allowed on any school machines.
- Files held on the schools' network are regularly checked.
- IT consultants will review system capacity regularly.
- Any administrator or master passwords for school IT systems are kept secure and available to at least two adults, e.g. the Headteacher. The password is changed regularly to maintain a high level of security.
- No-one except the IT consultants, Directors, and the Headteacher are allowed to download and install software onto the network.
- New users can only be given access by the IT consultants once permission is given by the Headteacher.
- Any laptops or school technology taken off school sites must be used in accordance with this and all other relevant school policies and any damage or loss is at the expense of the colleague.

NETWORK ACCESS

There are robust systems in place for managing network accounts and passwords, including safeguarding administrator passwords. Suitable arrangements are in place for visitors to the school who may be granted a temporary login. All users are provided with a log-in appropriate to their role within the schools and pupils are taught about safe practice about login and password information. All passwords are changed termly to maintain a high level of security and access to personal, private or sensitive information and data is restricted to authorised users only, with proper procedures being followed for authorising and protecting login and password information. Remote access to school systems is limited and covered by specific agreements and is never allowed to unauthorised third-party users. Guests or non-ABS colleagues are not given the Wi-Fi password unless a guest login is available.

EMAIL

Email is regarded as an essential means of communication and all employees are provided with an e-mail account. Communication by email should be related to school matters only. Email messages related to school matters should reflect a suitable tone and content, ensuring that the good name of the schools is maintained. The same procedures are expected of all other employees who send emails to external organisations. Use of the schools' e-mail system is monitored and checked and colleagues should not use personal email accounts during school hours or for professional purposes. Adults are not permitted to use school email accounts to communicate with pupils at any time. See our data protection policy for further information on use of email and storing documents on the drive.

PUBLISHING MATERIAL ONLINE AT ABS.UK AND PUPILS PUBLISHING ONLINE (BLOGS AND WEBSITES)

Achieve Beyond Schools maintains editorial responsibility for website content to ensure that the content is accurate, and the quality of presentation is maintained. The schools maintain the integrity of their website by ensuring that responsibility for uploading material is always moderated and that passwords are protected. The identities of pupils are always protected. Photographs of identifiable individual pupils are not published on the website unless parents/carers have provided written permission for the school to use pupils' photographs. Photographs never have names attached. In some instances, it may be appropriate for pupils to use websites or blogs to complete, or celebrate, their work. As always, the identities of pupils must be always protected. Photographs of identifiable individual pupils are not published unless parents/carers have provided written permission for the school to use pupils' photographs. Photographs must never have full names attached (first name or initials only) and no personal information that could be used to identify them should be disclosed. Parents/carers must have given specific permission via the user agreement forms to allow pupils to create websites or blogs.

OTHER ONLINE COMMUNICATION PLATFORMS

Adults and pupils are encouraged to adopt similar safe and responsible behaviour in their personal use of blogs, wikis, social networking sites and other online publishing inside and outside of school hours. Material published by pupils and colleagues in a social context which is considered to bring the schools' reputation into disrepute or considered harmful to, or harassment of, another child or member of the organisation will be considered a breach of conduct and behaviour and treated accordingly, as per our behaviour, equality, anti-bullying and/or people conduct policy/procedures.

USING IMAGES, VIDEO AND SOUND

Achieve Beyond Schools recognises that many aspects of the curriculum can be enhanced using multi-media and that there are now a wide and growing range of devices on which this can be accomplished. Pupils are encouraged and taught safe and responsible behaviour when creating, using, and storing digital images, video and sound through the following:

- Digital images, video and sound recordings are only taken with the permission of participants; images and video are of appropriate activities and are only taken of pupils wearing appropriate dress. Full names of participants are not used either within the resource itself, within the filename or in accompanying text online.
- All parents/carers are asked to sign an agreement about taking and publishing photographs and video of their pupils when offered a school or activity placement and this list is checked whenever an activity is being photographed or filmed.
- For their own protection, adults or other visitors to our premises are discouraged from using a personal device (mobile phone, digital camera, or digital video recorder) to take photographs of pupils or visitors.

MOBILE PHONES AND SMART WATCHES

Pupils are discouraged from bringing mobile phones and smart watches into school but if they do, they must hand them to the school offices for safe keeping until the

end of the school day. Adults are not to use mobile phones during the school day, except for calling the school or the emergency services if an emergency arises whilst off-site. They are not encouraged or expected to use personal mobile phones in any situation where their mobile phone number or other personal details may be revealed to a child or parent/carer. Unauthorised or covert use of a mobile phone or other electronic device, to record voice, pictures or video is strictly prohibited. The sending or forwarding of text messages deliberately targeting a person with the intention of causing them distress, 'cyber-bullying', will be considered a disciplinary matter for pupils and adults alike. The same is the case for other inappropriate use of mobile technology, such as 'sexting'. Pupils are taught about misuse of technology as a matter of course through the school's personal, social, health, economic education programme.

DATA (SEE OUR DATA PROTECTION POLICY)

The schools recognise their obligation to safeguard adults and pupils' personal data including that which is stored and transmitted electronically. We ensure:

- Pupils are taught about the need to protect their own personal data as part of their online safety awareness and the risks resulting from giving this away to third parties.
- Colleagues are provided with appropriate levels of access to the schools' management information systems which holds child data. Passwords are not shared and administrator passwords are restricted and kept securely.
- Colleagues are aware of their obligation to keep sensitive data secure when working on computers outside of school.
- When we dispose of old computers and other equipment, we take due regard for destroying information which may be held on them.
- Remote access to computers is restricted to teachers & leaders.
- There is full back up and recovery procedures in place for school data (all pupil and adult's data is kept securely online).
- Where sensitive adults or child data is shared with other people who have a right to see the information, for example professionals in social care teams, we label the material appropriately to remind them of their duty to keep it secure and securely destroy any spare copies.

All colleagues sign a contract which includes a confidentiality section when commencing work at Achieve Beyond Schools.

ONLINE SAFETY INCIDENTS

- All incidents, including online safety incidents, are recorded as per other incidents on our online MIS and safeguarding portal, as appropriate
- Any incidents where pupils do not follow the User Agreement will be dealt with following the school's behaviour policy and procedures
- In situations where a colleague is made aware of a serious online safety incident, concerning pupils, visitors or other colleagues, they will inform a leader who will respond in the most appropriate manner, according to the flowchart in Appendix 2
- Instances of cyber-bullying will be taken very seriously and will be dealt with using the schools' preventing and responding bullying procedures and the

organisation's disciplinary procedures. The organisation recognises that adults as well as pupils may be victims and will take appropriate action in either situation
- Incidents that create a risk to the security of the schools' network, or create an information security risk to the organisation, will be referred to the executive head. Appropriate advice will be sought and action taken to minimise any risks and prevent further instances occurring, including reviewing any policies, procedures or guidance
- If the action breaches school policy, appropriate sanctions will be applied. The schools will decide if parents/carers need to be informed if there is a risk that child data has been lost
- Achieve Beyond Schools reserves the right to monitor their premises' equipment and to search any technology equipment, including personal equipment with permission, when a breach of this policy is suspected

QUALITY ASSURANCE

Achieve Beyond Schools is led by a proprietor body, supported by an advisory panel. The proprietors ensure that they comply with their duties under legislation and fulfil their duty to remedy any weaknesses that are identified. In relation to online safety, duties and responsibilities include: The Education (Independent School Standards) Regulations apply a duty to proprietors of independent schools to ensure that arrangements are made to safeguard and promote the welfare of children. Members of the proprietor body have termly meetings with the Headteacher, who is responsible for ensuring effective safeguarding practices and compliance with the relevant ISS, including in relation to online safety and the effectiveness of the schools' filtering and monitoring systems are met in in full.

PUPILS' ONLINE ACCESS OUTSIDE OF SCHOOL, INCLDUING REMOTE LEARNING

Teachers are in regular contact with pupils' families. This communication is used, as necessary, to reinforce the importance of keeping their children safe online. Teachers may use Google Classroom as an online learning platform for the setting of work and for facilitating remote education. Our remote education provision reflects the NSPCC's helpful advice, 'Undertaking remote teaching safely'. We acknowledge that families are likely to find it helpful to understand what systems we use at ABS to filter and monitor online use. Teachers ensure that pupils' families are aware of what their children are being asked to do online in school and remotely, including the sites they are asked to access and who their child is going to be interacting with online.

NEW TECHNOLOGY

Achieve Beyond Schools will keep abreast of new technologies and consider both the benefits for learning and teaching and the risks from an online safety point of view. We will regularly review this policy to reflect any new technology that we use, or to reflect the use of new technology by pupils.