Ashgate Specialist Support Primary School
Crossacres Rd, Wythenshawe, M22 5DR
Tel:0161 359 5322 Fax: 0161 437 8601
email: admin@ashgate.manchester.sch.uk
Headteacher: Diane Wolstenholme B.Ed.Hons

Policy Statement:

19. eSafety Policy

Date policy written	March 2012
Reviewed, Consultation and Ratified	March 2012 March 2016 March 2017 November 2018
Review date	November 2019

INTRODUCTION

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. It provides instant access to a wealth of up-to-the minute information and resources from across the world, which would not ordinarily be available. Consequently, school need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies that children and young people are using both inside and outside of the classroom include:

- Websites
- Apps
- E-mail, Instant Messaging and chat rooms
- Social Media, including Facebook and Twitter
- Snapchat, Instagram, WhatsApp, Google+, Tumblr and Pinterest
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices including tablets and gaming devices
- Skype and Facetime
- Online Games
- Learning Platforms and Virtual Learning Environments
- Blogs and Wikis
- Podcasting
- Video sharing
- Downloading
- On demand TV and video, movies and radio / Smart TVs

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies and that some have minimum age requirements (13 years in most cases). The dangers associated with the Internet and emerging new technologies are well known, e.g. children and/or young adults might inadvertently access content of

an unsavoury, distressing or offensive nature on the Internet or receive inappropriate or distasteful emails.

At ***Ashgate Specialist Support Primary school,*** we understand the responsibility to educate our pupils on eSafety issues; teaching them the appropriate behaviours and skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom either with support or independently.

Everybody in the school community has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

Both this policy and the Acceptable Use Agreement (for all staff, governors, regular visitors [for regulated activities] and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, ipads, laptops, mobile devices and whiteboards etc); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones and other mobile devices).

As a school we believe that the benefits far outweigh the risks involved with the internet, staff and pupils are made aware of the issues and concerns and receive ongoing education / CPD in choosing and adopting safe practices and behaviours.

This policy is written in accordance with Manchester City Council guidelines. It focuses on each individual technology available within school and outlines the procedures in place to protect users and the sanctions to be imposed if these are not adhered to.

PROFESSIONAL RESPONSIBILITIES

When using any form of ICT, including the Internet, in school and outside school

For your own protection we advise that you:

- Do not talk about your professional role in any capacity when using social media such as Facebook and YouTube.
- Do not put online any text, image, sound or video that could upset or offend any member of the whole school community or be incompatible with your professional role.
- Use school ICT systems and resources for all school business. This includes your school email address, school mobile phone and school video camera.
- Do not give out your own personal details, such as mobile phone number, personal e-mail address or social network details to pupils, parents, carers and others.
- Do not disclose any passwords and ensure that personal data (such as data held on MIS software) is kept secure and used appropriately.

ROLES AND RESPONSIBILITIES

The Head Teacher of Ashgate Specialist Support Primary School will ensure that:

- All staff should be included in eSafety training. Staff must also understand that misuse of the internet may lead to disciplinary action and possible dismissal.
- A Designated Senior Member of Staff for E-Learning/Safety is identified and receives appropriate on-going training, support and supervision. (The designated person at Ashgate Specialist Support Primary School is Sophie Wood)
- A Designated member of the governing body will be identified to oversee eSafety (The designated person at Ashgate Specialist Support Primary School is Joan Holt).
- The Designated eSafety Officer should work closely with the Designated Person for Safeguarding if they are different members of the Senior Management team. (The Designated Safeguarding officers at Ashgate Specialist Support Primary School are Diane Wolstenholme and Sophie Wood).
- All temporary staff, visitors and volunteers are made aware of the school's eSafety Policy and arrangements.
- A commitment to eSafety is an integral part of the safer recruitment and selection process of staff and volunteers.
- Pupils, for whom it is deemed appropriate, will receive eSafety education / training as part of the school curriculum. Pupils will also be informed of the consequences for improper use of the internet.

The Governing Body of the school will ensure that:

- There is a senior member of the school's Leadership Team who is designated to take the lead on eSafety within the school.
- Procedures are in place for dealing with breaches of eSafety and security and are in line with Local Authority procedures.
- All staff and volunteers have access to appropriate ICT training / eSafety training.

The Designated Senior Member of Staff for E-Learning/Safety will:

- Act as the first point of contact with regards to breaches in eSafety and security.
- Liaise with the Designated Person for Safeguarding as appropriate.
- Ensure that ICT security is maintained through Infinity Computing.
- Ensure that IT security is maintained via support providers, Infinity Computing provide IT Support to school and One Education provide internet access along with filtering and firewall services.
- Attend appropriate training.
- Provide support and training for staff and volunteers on eSafety.
- Ensure that all staff and volunteers have received a copy of the school's eSafety Policy.
- Ensure that all staff and volunteers understand and are aware of the school's eSafety Policy.
- Ensure that the school's ICT systems are regularly reviewed with regard to security.
- Discuss security strategies with the Local Authority particularly where a wide area network is planned.
- Regularly check files on the school's network in conjunction with the IT administrator.

The IT Support provider (Infinity Computing) of the school will ensure that:

- Security patches/updates are applied to all devices where appropriate.
- Anti-virus protection is up to date and monitored.

- Accounts to IT systems are kept up to date and users have the correct level of access.
- Internet security is operational via the ISP (Internet Service Provider).
- Ensure only school equipment is connected to the school network.
- Security of the Wireless network.
- Prevent Radical Extremism.

TEACHING AND LEARNING

Benefits of internet use for education

The internet is a part of the statutory curriculum and a necessary tool for staff and children and young people and benefits education by allowing access to world - wide educational resources including art galleries and museums as well as enabling access to specialists in many fields for pupils and staff.

Access to the internet supports educational and cultural exchanges between students world - wide and enables pupils to participate in cultural, vocational, social and leisure use in libraries, clubs and at home.

The internet supports professional development for staff through access to national developments, educational materials, good curriculum practice and exchange of curriculum and administration data with the Local Authority and DCSF.

The internet improves access to technical support, including remote management of networks, supports communication with support services, professional associations and colleagues as well as allowing access to, and inclusion in, government initiatives.

The internet offers opportunities for mentoring pupils and providing peer support for them and their teachers.

Internet use will be planned to enrich and extend learning activities and access levels will be reviewed to reflect the curriculum requirements and age of the children and young people.

Cyber Bullying, Sexting, Peer on Peer Abuse and Banter

Staff should:

- All be aware of the guidance given in **Keeping Children Safe in Education September 2016** on specific types of abuse found in Annex A of the document

  https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/741314/Keeping_Children_Safe_in_Education__3_September_2018_14.09.18.pdf

  A paper copy of this document is in every classroom and in the school office for reference.
- Recognise that children are capable of abusing their peers
- Recognise that children may be a victim of abuse from peers and that children with SEND are particularly vulnerable to this.
- Challenge any form of derogatory and sexualised language or behaviour

- Be vigilant to sexualised/aggressive touching or grabbing

Concerns should be reported to senior staff who will consult with the designated safeguarding lead (DSL). Victims of peer abuse, including sexting, should be supported by the school staff and referred to relevant specialist agencies where appropriate.

The school's curriculum will

- Be adapted to meet the needs and level of understanding of individual children.
- Teach children to recognise appropriate and inappropriate behaviours
- Support pupils to become more resilient to inappropriate behaviours towards them, risk-taking behaviours, and behaviours that children may be coerced into, including sexting.
- Teach them how to report inappropriate behaviour and seek help
- Inform and involve parents in understanding how to keep their children safe from this type of abuse.

AUTHORISING INTERNET ACCESS

All staff must read the school's eSafety Policy. All staff and visitors must sign AUP agreement before accessing the internet.

PROCEDURES FOR THE USE OF A SHARED NETWORK

All staff and visitors using the school network must follow these agreed procedures:

- Users must access the network using their own logons and passwords. These must not be disclosed or shared.
- On termination of employment, resignation or transfer, all ICT equipment will be returned to Senior Management. IT Support need to be informed so that all relevant accounts can be disabled, any IT equipment such as laptops or tablets are to be returned to IT Support for checking before they are re-allocated.
- Procedures are in place on the network system to ensure users change their passwords regularly.
- If a member of staff forgets their password they need to log a support request to the Support company for it to be reset.
- Pupils log on as their own class and passwords are not used at the present time. This will be reviewed and adapted as appropriate.
- Users must respect confidentiality and attempts should not be made to access another individual's personal folder on the network without permission. At Ashgate Specialist Support Primary School the Senior Management team and IT Administrator (Infinity Computing) have authority to access all areas of the school intranet.

- Software should not be installed without prior permission from the person responsible for managing the network. (Please speak to IT Technician) This also applies to Laptops used off site.
- Personal removable media (e.g. pen drives / memory sticks and CD-ROMs) must not be used on school network/laptops. School devices may be used on school premises.
- Only approved online storage should be used to store files relating to school work, guidance should also be followed regarding what files should not be saved to online storage and must only be kept on the internal school network.
- Machines must never be left 'logged on' and unattended. If a machine is to be left for a short while, it must be 'locked.' (Ctrl+alt+del followed by 'lock computer').
- Machines must be 'logged off' correctly after use.
- SLT, admin staff and teachers may access the school's network securely by using "LogMeIn" – this will be monitored by IT Technician and login details must be kept confidential and guidance notes followed.
- Ashgate Specialist Support Primary School will retain archived photos of ex-pupils for 8 years. Regular monitoring to comply with Data Protection laws will take place in the Summer term.

WIRELESS NETWORK

It is the responsibility of the IT Technician to maintain the wireless network in school. The wireless network must be encrypted to prevent outsiders from being able to access it.

The encryption code will be known only to IT Technician and SLT and must not be divulged. Every effort will be made to maintain security of access code and the code will be changed if network security is compromised. Passwords will be stored securely in IT Technician's office.

MANAGING INTERNET ACCESS

Developing good practice in internet use for teaching and learning is essential. Ashgate Specialist Support Primary School's internet access will be designed expressly for pupils use and will include filtering appropriate to the needs and capabilities of the children and young people.

Pupils will be taught / supported to gain a better understanding of what internet use is acceptable and what is not and be given clear objectives for internet use. Staff will guide pupils in on-line activities that will support the learning outcomes planned. Statements based on ability levels rather than age will be available in accessible formats (adapted from Childnet's SMART Rules: www.childnet.com) to support them to make good choices when using the internet.

Through the SMART rules pupils will be taught what to do if they experience material that they find distasteful, uncomfortable or threatening.

If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the designated Esafety officer.

The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.

MANAGING EMAIL

School email addresses are available for Teachers, TAs and admin staff, any school related communications should only be made via official school email addresses (see ICT Subject Leader or ICT Technician).

Users must access the internet and email using their own logon / password and not those of another individual. Passwords must remain confidential and no attempt should be made to access another user's email account.

The internet and school email must only be used for professional, CPD or educational purposes.

Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information.

Staff may access personal emails in designated break / lunch times. Staff are reminded that whilst on school premises and using school hardware school policy and procedures remain the same.

Access in school to external personal e-mail accounts may be blocked.

Personal e-mail or messaging between staff and pupils should not take place.

Staff must use the school e-mail address if they need to communicate with pupils /parents about their school work / day as in the home school diary.

Pupils and staff may only use approved e-mail accounts on the school system and pupils must inform a member of staff immediately if they receive an offensive e-mail. Whole –class or group e-mail addresses should be used on the ipad ONLY.

Email addresses assigned to pupils will not be in a form which makes them easily identifiable to others. IT Technician will monitor use / content of emails by pupils. Pupils will only send and receive emails internally.

Pupils must not disclose any information of a personal nature in an email or on the Internet. This includes mobile and home phone numbers, addresses, or anything else which might allow them to be identified.

Excessive social e-mail use can interfere with learning and will be restricted.

All staff should remember emails are not fully secure, if any confidential or identifying data must be sent via email it must be encrypted using Egress.

The forwarding of chain letters is not permitted.

All emails sent should be courteous and the formality and tone of the language used appropriate to the reader. No strong or racist language will be tolerated. Sanctions, appropriate to the case, will be imposed on any users who break this code.

Bullying, harassment or abuse of any kind via email will not be tolerated. Sanctions, appropriate to the case, will be imposed on any users who break this code.

If users are bullied, or offensive emails are received, this must be reported immediately to the SLT or Governors within the school. Emails received should not be deleted, but kept for investigation purposes.

Anti-virus software is used on all machines and this is regularly updated to ensure its effectiveness.

Users must be aware of potential threats/hazards caused by downloading files from the Internet. Users must only download files for educational purposes and consult IT Technician / eSafety Officer if in doubt.

PROCEDURES FOR THE USE OF INSTANT MESSAGING (IM), CHAT AND WEBLOGS

(e.g. Twitter, Facebook, MSN, Bebo, Linkedin, Pinterest, Google+ Tumblr, Instagram, Flickr, VK, Myspace, Tagged, Meetup, Ask.fm) is not permitted in school.

Staff should not use Facetime, Skype or social networking sites (e.g. “Facebook”) or personal publishing (e.g. “Blogs”) for discussing or commenting on any school activities e.g. planning, meetings, lessons etc.

As members of staff and other professionals work remotely, Facetime, Skype, Zoom and Microsoft Teams etc have become invaluable for enabling people to meet and stay connected at a time when social distancing and shielding is in place. School related matters may therefore be discussed on these forums.

When conducting virtual meetings, confidentiality should be maintained at all times, ensuring that those invited need to be privy to the agenda and that the conversation remains private from other members of the household, in a separate room.

Please follow the same rules that you would in face to face meetings, whereby that you treat each other in a respectful and professional manner.

Those hosting the meeting may arrange for microphones to be turned on/off to avoid interruption to the speaker. Members of staff may be asked to signal with a hand gesture when they would like to speak so that all points of view are heard.

Staff should not use social media for discussing or commenting on colleagues, pupils, parents, or reference any other links with Ashgate. This includes mentioning Ashgate School on profile pages on social media.

Staff may publicise fundraising events and donate pages which they are involved in for Ashgate School and / or charities, once they have gained permission from SLT.

For the protection of their own professional security, staff are advised to ensure that appropriate high privacy settings are applied and consider if posts, comments, images, links and videos shared on a profile are appropriate and transparent.

Staff using social media (facebook, twitter, myspace, youtube) should ensure that any comments, photos and videos posted or ‘liked’:

* Do not bring the school into disrepute

* Do not bring the staff member into disrepute

* Do not expose the school to legal liability

* Reflect ‘safer internet’ practices

* Minimise risks associated with the personal use of social media by professionals and

* Reflects the school’s standard of behaviour and staff code of conduct.

* Reflect the school’s ethos relating to staff wellbeing and consider other people’s feelings. Education is a topic which is being widely discussed in the media. Please be mindful when responding to the news that everybody has different opinions, circumstances and perspectives and therefore, how your posts may be perceived and interpreted. Consider your wider audience, e.g. parents, friends, colleagues and whether these comments are shared in a private conversation or in a public forum.

Children/Young adults and staff must not access public or unregulated chat rooms.

If staff are approached by pupils, past pupils or parents to ‘connect’ with them online e.g. through the use of friend requests, staff are to decline and seek further advice from Senior Management if required. The exception to this would be if the parent is employed by Ashgate School or the link is made via the Friends of Ashgate Facebook Page. Under these circumstances, the member of staff who had been approached by the parent to ‘connect’ with them online would discuss in person that they are able to accept the request as they would both be following the same guidelines of the eSafety policy.

Pupils and parents will be advised that the use of social network sites outside school is inappropriate for primary aged pupils.

For Professional Development purposes, staff are permitted and indeed encouraged to use interactive media, e.g. SLD Forum etc. However, staff are reminded to retain confidentiality on these sites and to ensure that no individual pupil is identifiable. In these instances staff are advised to use personal email addresses so that the school is not identifiable.

WhatsApp and private messaging has also been utilised as a way to share information relating to school and communicate quickly with a number of different people, e.g. the Lunchtime Organiser WhatsApp group which focuses of checking availability for cover.
As is the case with emails, these messages should also reflect the positive, professional ethos of the school. Messages sent should be courteous and the tone of the language, appropriate to the reader. Where possible, messages should be sent and replied to during the working day, unless it is a matter of urgency.

PROCEDURES FOR THE USE OF CAMERAS AND VIDEO EQUIPMENT

Permission must be obtained from a child's parent or carer before photographs or video footage can be taken. A central record of permissions given will be kept on the shared area, staff full – ICT – photograph consent (academic year).

Photographs or video footage will be downloaded immediately and saved onto the media drive. The media drive will be protected via password log-on and accessible only to authorised members of staff.

Any photographs or video footage stored must be deleted immediately once no longer needed. Class teachers will be responsible for collating key photos of each child in a folder at the end of the academic year. This folder will be transferred to the child's next teacher and any unwanted photos will be deleted. When the pupil reaches the end of Year 6, their folder of photographs will be archived by Infinity Computing and stored for 8years before being deleted.

Any adult using their own camera, video recorder during a trip or visit must receive permission from a member of SMT and transfer and save images and video footage into the password protected media drive in school immediately upon their return.

It is not appropriate to use photographic or video technology in toilets, hygiene suites, swimming pools and changing rooms.

Audio or video files may only be downloaded if they relate directly to the current educational task being undertaken. Staff should be aware that the downloading of music or video files may take up significant bandwidth (capacity) on the school network or its internet connection. This may slow the network down or in severe cases cause the network or the internet connection to fail.

PROCEDURES TO ENSURE THE SAFETY OF THE SCHOOL WEBSITE

The school has designated members of staff (Head Teacher / IT Technician) who are responsible for approving all content and images to be uploaded onto its website prior to it being published.

The school website will be subject to frequent checks to ensure that no material has been inadvertently posted, which might put children or staff at risk.

Copyright and intellectual property rights must be respected.

Permission must be obtained each new academic year from parents or carers before any images of children can be uploaded onto the school website.

Names must not be used to identify individuals portrayed in images uploaded onto the school website, photographs which might enable this individual to be identified must not appear. Permission must be sought from staff members if names are used on the website (SLT).

When photographs to be used on the website are saved, names of individuals should not be used as file names.

The website is password protected. Staff of Ashgate School must not share their login or password with anyone else.

The eSafety Officer and Head Teacher will take overall editorial responsibility and ensure content is accurate and appropriate.

The copyright of all material must be held by the school, or to be attributed to the owner where permission to reproduce has been obtained.

PROCEDURES FOR USING MOBILE PHONES AND PERSONAL DIGITAL ASSISTANTS (PDA'S) IN SCHOOL

Staff

Staff are to switch mobile phones to silent / off during normal school hours and store in personal lockers, locked drawer, handbag or locked stockrooms.

Staff may access their mobile phones at break / lunchtimes but may only use them in recognized office spaces, the staff room, areas that are private and free from children or off school premises.

Mobile phones must not be taken into hygiene or changing areas under any circumstances.

Staff may not use their mobile phone to take still pictures or video footage of children in school or on Educational visits.

Staff must not take still pictures of video footage of other adults in school without the subject's permission.

Staff must not use a mobile / camera phone for inappropriate or malicious purposes, e.g. the sending of abusive or unsavoury images / text messages or the making of hoax, crank or abusive phone calls, etc. Any incidents must be reported without delay to the person responsible for eSafety.

If Staff or children do receive unwanted or hurtful calls or text messages, **they** should report incidents without delay to the person responsible for eSafety. (N.B. Any such messages should not be deleted nor replied to).

Staff should not access inappropriate websites and content via their mobile phones or PDA and must not do so whilst on school property.

Specific staff may be authorised by the Head teacher to carry and use school mobile phones whilst on site due to the complex needs of the pupils they are supporting, e.g. PMLD pupils with complex medical needs, e.g. when in soft play, the group room, hydrotherapy pool, sensory room or Nurture.

Specific staff may be authorized by the Head teacher to carry and use personal mobile phones whilst on school premises, e.g. members of the Senior Leadership Team.

Visitors.

Specific Visitors to the school are to be informed of the school's eSafety policy.

Visitors must sign to indicate that they understand and agree to abide by agreed policies and procedures when in school.

Visitors who may need to access their phones during the course of their visit must do so in an appropriate location, e.g. office / staff room.

Visitors needing to use school computers must not use staff log-in to access school network/internet. They must seek permission from Office Staff and use a separate login.

PROCEDURES FOR USING MOBILE PHONES AND PERSONAL DIGITAL ASSISTANTS (PDA'S) OFF SITE

Staff are to use school mobile phones when offsite with pupils on Educational Visits.

On full day Educational visits / Residential visits staff may take personal mobiles with them as long as they are switched off/on silent and only accessed during agreed break times away from the pupils.

On full day / Residential visits specific staff may be authorized by the head teacher to use personal mobile phones in support of school mobile phones due to the complex needs of the pupils they are supporting, e.g. PMLD pupils with complex medical conditions or ASC pupils with Behaviour Support Plans.

PROCEDURES FOR THE USE OF WIRELESS GAMES CONSOLES

Pupils may use wireless games consoles whilst in school, e.g Wii. They must not use the internet to play games online.

PROCEDURES FOR THE USE OF PORTABLE MEDIA (E.G. IPODS)

As a general rule pupils must not use Portable media players (e.g. iPods) in school. Exceptions to this are at the discretion of the Head teacher e.g. in support of a Behaviour Support Plan.

Staff wishing to use Portable media players (e.g. iPods) in school must only do so in recognised break time and in approved location, e.g. Staffroom or during assembly.

Any misuse of portable media players to be reported to the person responsible for eSafety.

Concerns relating to eSafety

Any misuse or abuse of either the school's internet or technology will be taken very seriously and may lead to disciplinary action being taken. Any incidents of misuse will be considered on an individual basis by the Head teacher and Senior Management Team.

Complaints of Internet misuse will be dealt with by a senior member of staff.

Any complaint about staff misuse must be referred to the Head teacher.

Complaints of a child protection nature must be dealt with in accordance with school child protection procedures and reported via CPOMS.

Where appropriate, pupils and parents will be informed of the consequences for pupils of misusing the Internet. Letters may be sent home to parents or carers (if applicable).

ENLISITING PARENTS SUPPORT

Parent's attention will be drawn to the school eSafety Policy in newsletters, on the school website and during school meetings. They will be asked not to publish any photographs online which they take at the Summer / Christmas Concert.

A partnership approach to eSafety at home and at school with parents will be encouraged. This may include offering meetings and coffee mornings with demonstrations and suggestions for safe home Internet use, or highlighting eSafety at other attended events e.g. parents evenings.

Internet issues will be handled sensitively and parents will be advised accordingly.

The school will compile a list of eSafety resources in a variety of formats which can be used by staff or parents with pupils. Advice on useful resources and websites, filtering systems and educational leisure activities which include responsible use of the Internet will be made available to parents.

CONCLUSION

The procedures in this policy will be subject to ongoing review and modification in order to keep up with advances in the technology coming into school. This policy will not remain static. It may be that staff / children might wish to use an emerging technology for which there are currently no procedures in place consequently the use of any emerging technologies will be permitted upon completion and approval of a risk assessment, which will be used to inform future policy updates. The school will audit ICT use to establish if the eSafety policy is adequate and that the implementation of the eSafety policy is appropriate and effective.