ASTON TOWER COMMUNITY PRIMARY SCHOOL

E-Safety Policy

Our Vision:

Aston Tower Community Primary School embraces the positive impact and educational benefits that can be achieved through appropriate use of the Internet and associated communications technologies. We are also aware that inappropriate or misguided use can expose both adults and young people to unacceptable risks and dangers. To that end, Aston Tower Community Primary School aims to provide a safe and secure environment which not only protects all people on the premises, but also educates them on how to stay safe in the wider world.

Scope:

This policy and related documents apply at all times to fixed and mobile technologies owned and supplied by the school and to personal devices owned by adults and young people while on the school premises.

Related Documents:

Acceptable Use Policy for Adults

Safeguarding

Acceptable Use Policy for Young People

Anti-bullying Policy

Birmingham City Council Internet Use Policy, Internet Use Code of Practice and Email Use Policy (linked from www.bgfl.org/esafety)

AUP's in context: Establishing safe and responsible behaviours

Policy Owner (DSL and e-Safety Co-ordinator): Devinder Kaur

Implementation Date: November 2015

Publicising e-Safety:

Effective communication across the school community is key to achieving the school vision for safe and responsible citizens. To achieve this we will:

- Make this policy, and related documents, available on the school website at: http://www.astontowerprimary.co.uk
- Introduce this policy, and related documents, to all stakeholders at appropriate times. This will be at least once a year, or whenever it is updated
- Post relevant e-Safety information in all areas where computers are used
- Provide e-Safety information at parents evenings and through the school newsletter

Roles and Responsibilities

The Head and Governors have ultimate responsibility for establishing safe practice and managing e-Safety issues at our school. The role of e-Safety co-ordinator has been allocated to Devinder Kaur, our Designated Safeguarding Lead (DSL) for child protection and a member of the senior management team. They are the central point of contact for all e-Safety issues and will be responsible for day to day management. The school has established an e-Safety committee that are responsible for policy review, risk assessment, and e-safety in the curriculum. The current members are: The Computing Curriculum Leader, Abdul Hasnat (Systems Manager) and Deborah Ward (Business Manager) and Devinder Kaur (DSL).

All members of the school community have certain core responsibilities within and outside the school environment. They should:

- Use technology responsibly
- Accept responsibility for their use of technology
- Model best practice when using technology
- Report any incidents to the e-Safety coordinator using the school procedures
- Understand that network activity and online communications are monitored, including any personal and private communications made via the school network.
- Be aware that in certain circumstances where unacceptable use is suspected, enhanced monitoring and procedures may come into action

Physical Environment / Security

The school endeavours to provide a safe environment for the whole community and we review both physical and network security regularly and monitor who has access to the system consulting with the LA where appropriate.

- Anti-virus software is installed on all computers and updated regularly
- Central filtering is provided and managed by Link2ICT. All staff and pupils understand that if an inappropriate site is discovered it must be reported to the e-Safety co-ordinator and the Information Systems Manager who will report it to the Link2ICT Service Desk to be blocked. All incidents will be recorded in the e-Safety log for audit purposes.
- Requests for changes to the filtering will be directed to the Headteacher in the first instance who will forward these on to Link2ICT. Change requests will be recorded in the e-Safety log for audit purposes
- The school uses Policy Central Enterprise on all school owned equipment to ensure compliance with the Acceptable Use Policies.
    - Pupils use is monitored by Abdul Hasnat
    - Staff use is monitored by the Head.
- All staff are issued with their own username and password for network access. Visitors / Supply staff are issued with temporary ID's and the details recorded in the school office.
- Key stage one pupils use class logon IDs for their network access
- Key stage two pupils have their own username and password and understand that this must not be shared.

All pupils in KS2 issued with their own username and password and understand that this must not be shared with anyone.

Mobile technologies

- Teaching staff at the school are provided with a laptop for educational use and their own professional development. All staff understand that the Acceptable Use Policies apply to this equipment at all times, on and off the premises and irrespective of the network being used to provide internet access.
- To ensure the security of the school systems, personal equipment is currently not permitted to be connected to the school network.
- Staff understand that they should use their own mobile phones sensibly and in line with school policy.
- Pupils understand that their mobile phones must not be brought into school, except in extenuating circumstances and at the discretion of the Head Teacher.
- The Educations and Inspections Act 2006 grants the Head the legal power to confiscate mobile devices where there is reasonable suspicion of misuse and the Head will exercise this right at their discretion
- Pictures / videos of staff and pupils must not be taken on personal devices.

E-mail

The school e-mail system is provided, filtered and monitored by Office 365 and is governed by Birmingham City Council E-mail Use Policy

- All staff are given a school e-mail address and understand that this must be used for all professional communication
- Pupils have access to class based e-mail accounts that are monitored by the class teacher
- Staff are allowed to access personal e-mail accounts on the school system outside directed time and understand that any messages sent using the school equipment should be in line with the e-mail policy. In addition, they also understand that these messages will be scanned by the monitoring software
- Pupils may be given the opportunity to check their own e-mail outside directed time and understand that any messages sent using the school equipment will be scanned by the monitoring software.
- Everyone in the school community understands that any inappropriate e-mails must be reported to the class teacher / e-Safety co-ordinator as soon as possible
- The school will help the wider school community (including parents, carers and guardians) to understand what reporting arrangements exist for serious and persistent misuse of email systems, including cyber bullying.

Published content

The Head takes responsibility for content published to the school web site but has delegated general editorial responsibility to Deborah Ward. Class teachers and Key Stage co-ordinators are responsible for the editorial control of work published by their Pupils.

- The school will hold the copyright for any material published on the school web site or will obtain permission from the copyright holder prior to publishing with appropriate attribution.
- The school encourages the use of e-mail to contact the school via the school office / generic e-mail addresses / staff e-mail addresses
- The school does not publish any contact details for the pupils
- The school encourages appropriate, educational use of other Web 2.0 technologies and where possible embeds these in the school web site or creates a school account on the site
- Any content published on Twitter must first be approved by the Head Teacher.

Digital Media

We respect the privacy of the school community and if parents do not wish for their child's likeness to be included in content published online, written confirmation of this will be obtained.

Published photographs will not identify any individual pupil

- Pupils' full names will not be published outside the school environment
- Written permission will be obtained from parents or carers prior to pupils taking part in external video conferencing.
- Pupils understand that they must have their teachers permission to make or answer a video conference call
- Supervision of video conferencing will be appropriate to the age of the pupils

Social Networking and online communication

The school does not allow access to social networking websites with the exception of Twitter (for details on appropriate content see Published Content)

Guidance is provided to the school community on how to use these sites safely and appropriately. This includes

- not publishing personal information
- not publishing information relating to the school community
- how to set appropriate privacy settings
- how to report issues or inappropriate content

Unmoderated chat sites present an unacceptable level of risk and are blocked in school. Pupils are given age appropriate advice and guidance around the use of such sites

Educational Use

School staff model appropriate use of school resources including the internet.

- All activities using the internet, including homework and independent research topics, will be tested first to minimise the risk of exposure to inappropriate material
- Where appropriate, links to specific web sites will be provided instead of open searching for information
- Pupils will be taught how to conduct safe searches of the internet and this information will be made available to parents and carers
- Teachers will be responsible for their own classroom management when using ICT equipment and will remind pupils of the Acceptable Use Polices before any activity.
- Staff and pupils will be expected to reference all third party resources that are used
- Where computer and video game technology is used for clubs or educational purposes, all software must be checked for appropriate content before use.

E-safety training

The school have completed a baseline assessment of current staff skills and have a program of continuing professional development in place that includes whole school inset, in school support, consultancy and course attendance.

- All new members of staff to be provided with a copy of this policy and any follow up questions to be directed to the DSL/e-safety co-ordinator
- Educational resources are reviewed by subject co-ordinators and disseminated through curriculum meetings / staff meetings / training sessions
- E-Safety is embedded throughout the school curriculum and visited by each year group as part of the programme of study bought in by the school (2014/15)
- Pupils are taught how to validate the accuracy of information found on the internet
- Parents sessions are available to provide appropriate advice and guidance

Data Security / Data Protection

Personal data will be recorded, processed, transferred and made available in line with the Data Protection Act 1998

Data is stored on the school systems and transferred in accordance with the Becta Data Security Guidelines

Wider Community

Third party users of school equipment will be advised of the policies, filtering and monitoring that is in place. They will be issued with appropriate usernames and password that will be recorded in the school office.

Responding to incidents

Inappropriate use of the school resources will be dealt with in line with other school policies e.g. Behaviour, Anti-Bullying and Child Protection Policy.

- Any suspected illegal activity will be reported directly to the police. The Link2ICT Service Desk will also be informed to ensure that the Local Authority can provide appropriate support for the school
- Third party complaints, or from parents concerning activity that occurs outside the normal school day, should be referred directly to the Head
- Breaches of this policy by staff will be investigated by the head teacher. Action will be taken under Birmingham City Council's Disciplinary Policy where a breach of professional conduct is identified. Incidents will be fully investigated and appropriate records made on personal files with the ultimate sanction of summary dismissal reserved for the most serious of cases involving gross misconduct. All monitoring of staff use will be carried out by at least 2 senior members of staff.
- Student policy breaches relating to bullying, drugs misuse, abuse and suicide must be reported to the nominated child protection representative and action taken in line with school anti-bullying and child protection policies. There may be occasions when the police must be involved.
- Serious breaches of this policy by pupils will be treated as any other serious breach of conduct inline with school Behaviour Policy. Referral to Heads of Phase may be appropriate at this level. Heads of Phase will also deal with email alerts generated by PCE for pupils. For all serious breaches, the incident will be fully investigated, and appropriate records made on personal files with the ultimate sanction of exclusion reserved for the most serious of cases.
- Minor student offenses, such as being off-task visiting games or email websites will be handled by the teacher in situ by invoking the school behaviour policy.
- The Educations and Inspections Act 2006 grants the Head the legal power to take action against incidents affecting the school that occur outside the normal school day and this right will be exercised where it is considered appropriate