Ark Boulton Academy

"Growing together, reaching higher"

E-SAFETY GUIDANCE

Including cyber-bullying & images

2016 - 2017

CONTENTS

1. PRINCIPLES

We teach our children to swim not just to prevent them from drowning but also for the pleasure they may get from it and the benefits it brings to their health. Similarly, we must teach children to 'swim' in the online world not only to ensure their safety but also to enable them to improve their emotional health and their enjoyment of the world.

E-safety is always about balancing opportunities with risks and we believe as firmly in maximising opportunities as in minimising risks. We must encourage children and young people to develop as responsible online citizens. Such citizens will recognise their responsibility to keep themselves and their peers safe online, but they will also recognise the responsibility they have to present themselves as positive role models. It is only through the development of a sense of online responsibility that we can ensure the safety and well-being of today's children and young people.

All of the 'staying safe' aims apply equally to the 'virtual world' that children and young people will encounter whenever they use ICT in its various forms. For example, we know that the internet has been used for grooming children and young people with the ultimate aim of exploiting them sexually, we know that ICT can offer new weapons for bullies, who may torment their victims via websites or text messages, and we know that children and young people have been exposed to inappropriate content when online, which can sometimes lead to their involvement in crime and anti-social behaviour.

It is the duty of the academy to ensure that every child in their care is safe, and the same principles should apply to the 'virtual' or digital world as would be applied to the academy's physical buildings.

This policy document is drawn up to protect all parties, the students, the staff and the academy and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements. It also outlines how we will educate pupils, parents and staff in the safe use of the internet and information technology.

2. PURPOSE

Ark Boulton Academy aims to provide a learning environment with the highest opportunities for children to achieve their full potential. As part of this aim we see access to the internet as a powerful tool.

We believe that access to the internet:

- Enriches the quality of curriculum provision and extend learning activities.
- Helps us raise children's attainment.
- Supports teachers' planning and resourcing of lessons.
- Enhances the academy's management and administration systems.
- Enhances staff development through access to educational materials, as well as the sharing of information and good curriculum practice between academies, support centres, the LEA and DFE.

However, it is also the case that the use of such technology may sometimes expose children to the risk of harm.

Apart from the risk of children accessing internet sites which contain unsuitable material, risks to the well-being of children may also exist in a variety of other ways

This policy therefore details strategies and guidance for addressing the issues of:

- Publishing digital images of students and staff.
- Keeping children safe from grooming via the internet or other digital communication devices.
- Keeping children safe from cyber bullying.
- Keeping children safe from inappropriate digital content.
- Keeping teaching staff and other adults safe.

General principles for dealing with e-safety issues:

- An environment should be encouraged where students feel confident when it comes to reporting inappropriate incidents involving the internet, mobile technology or email.
- Ark Boulton Academy makes use of an effective range of technological tools to maintain a safe ICT learning environment.
- Roles and responsibilities of staff involved are clearly designated and monitored. The network manager and the designated teachers will investigate and take appropriate action where there are safeguarding concerns.
- The academy will deliver an on-going education programme for students, staff and parents.
- Keeping children safe from internet grooming.

If there is concern that a child's safety is at risk because there is a suspicion that someone is using communication technology (such as social networking sites) to make inappropriate contact with a child, then the concern should be reported to and discussed with one of the named Safeguarding Officers in the academy.

If appropriate the following could be actioned:

- A decision made as to whether parents should be contacted.
- Advise the child on how to terminate the communication and save all evidence.
- Contact Child Exploitation & Online Protection http://www.ceop.gov.uk.
- Consider the involvement of police and social services.

To safeguard students the academy:

- Blocks all chat rooms and social networking sites (that we are aware of or made aware of) except those that are part of an educational network.
- Only uses approved and appropriate blogging or discussion sites.
- Only uses approved or checked webcam sites.

3. KEEPING CHILDREN SAFE FROM CYBER BULLYING

Ark Boulton Academy will not tolerate bullying, whatever form it takes. Bullying is when a person is deliberately hurt or made to feel unhappy. It is sustained and involves an imbalance of power. Cyber bullying is bullying through the use of communication technology like mobile phone text messages, e-mails or websites. This can take many forms for example:

- Sending threatening or abusive text messages or emails, personally or anonymously.
- Making insulting comments about someone on a website, social networking site (e.g. Facebook, MySpace), web blog or messaging system.
- Making or sharing derogatory or embarrassing images, videos or audio of someone via mobile phone, email or website (such as 'Happy Slapping' videos or 'sexting').

Using ICT to bully could be against the law. Abusive language or images, used to bully, harass or threaten another, whether spoken or written (through electronic means) may be libellous, and may contravene the Harassment Act 1997 or the Telecommunications Act 1984.

If a bullying incident directed at a child occurs using email, website, blog or mobile phone technology and is in any way connected to the academy:

- Advise the child not to respond to the message.
- Refer to relevant policies including e-safety and Behaviour and Ethos, and apply appropriate sanctions.
- Secure and preserve any evidence.
- Inform the sender's e-mail service provider.
- Notify parents of the children involved.
- Consider delivering a parent workshop for the academy community.
- Consider informing the police depending on the severity or repetitious nature of offence.

If malicious or threatening comments are posted on an Internet site about a pupil or member of staff inform a member of SLT who will:

- Request the comments be removed if the site is administered externally.
- Secure and preserve any evidence.
- Internally investigate the incident and inform the Principal.

The academy should then consider:

- Sending all the evidence to CEOP at www.ceop.gov.uk/contact_us
- Endeavouring to trace the origin and inform police as appropriate.
- Informing the Birmingham LSCB.

4. KEEPING CHILDREN SAFE FROM INAPPROPRIATE INTERNET CONTENT

This academy:

- Supervises pupils' use at all times, as far as is reasonable, and is vigilant in learning resource areas where older pupils have more flexible access.
- We use programmes which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature.
- Encourages staff to preview all sites before use (where not previously viewed and cached) or only use sites accessed from managed 'safe' environments.
- Plans the curriculum context for Internet use to match pupils' ability, using a filtering system to minimise the risk to users when searching the internet.
- Informs users that Internet use is monitored.
- Informs staff and students that that they must report any failure of the filtering systems directly to the ICT Network Manager who will report to the Senior Staff and outside agencies such as the Local Authority where necessary.
- Will block pupil access to music download or shopping sites as we become aware of the, except those approved for educational purposes.
- Requires all staff to agree to an e-safety agreement when they log onto their computer.
- Makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse through staff meetings and teaching programme.

- Keeps a record, e.g. print-out, of any bullying or inappropriate behaviour for as long as is reasonable in-line with the academy behaviour management system.
- Will refer any material we suspect is illegal to the appropriate authorities (LA /Police) once a thorough internal investigation has taken place.

5. KEEPING TEACHERS AND OTHER ADULTS SAFE

Infringements of E-Safety Policy do not only involve students. There are increasing incidents of teachers and other adults working in education being the victims of 'cyber bullying'.
In order to minimise the risk the Academy strongly recommends that you:

- Only use the academy email and academy telephone system to communicate with students, staff and parents.
- Do not share (with students or parents) any personal contact details such as home addresses, personal phone numbers or email accounts. For academy trips always borrow an academy mobile phone.
- Consider carefully how you use social networking sites including privacy settings and accessibility, ensuring that students or parents cannot access personal information, including photographs.
- Do not invite students or parents to be 'friends' on social networking sites.
- Do not accept invitations to become members of students' or parents' networking sites.
- If colleagues choose to disregard the above advice the academy may not be able to protect them from the consequences.

6. IMAGES – ACCEPTABLE USE POLICY

This policy covers the publishing of digital images of students and staff in paper based documents, on the academy's website, via email or using removable storage devices. It includes both still and moving images, video and audio files.

The academy does not allow images of its students and staff to be published on third party websites (i.e. YouTube) unless written permission has been granted. If a pupil or a member of staff uses third party websites to undermine or bully other members of the academy, they will be sanctioned accordingly.

The academy will use digital images of students and staff where it feels it is appropriate to do so. Examples of where they might be used are:

- To celebrate achievement.
- To promote the academy and its work.
- To improve the quality of the learning experience.

When using any digital image the academy will ensure that the person's privacy is protected. It will do this by:

- Having the student's permission to publish. This is done through the signing of the home-academy agreement.
- Not publishing (print or digital) the student's name in a way that could link the name to the image except where parental permission is obtained.
- Not publishing any personal/sensitive details. When storing digital media (images, video or audio files) of students or staff within the academy they will be stored safely on a staff area on the academy's network.

7. DATA PROTECTION

Sensitive information about pupils and staff should only be viewed by staff whilst on site and only kept on record for the required period of time in accordance with the Data Protection Act. If a member of staff needs to view this information offsite, staff should use an encrypted/password protected device or software. They should also clear this with their line manager.

8. EDUCATION AND TRAINING

Students

- Regular assemblies.
- Education through PSHE lessons.
- Distributing any appropriate leaflets or promotional material provided by external organisations such as CEOP, Safe, Digital Me.

Staff

- Regular reminders and guidance using staff meetings, email, staff bulletin, and website.
- Annual requirement to read and sign off ICT policy.

Parents and other adults

- Policy and guidance included in Home /School agreement signed by all parents.
- Articles in academy newsletter.
- Flagging of policies and procedures on Academy website.
- Information evenings.

9. GUIDANCE - WHAT DO WE DO IF?

N. B. Children should be confident in a no blame culture when it comes to reporting inappropriate incidents involving the internet or mobile technology. They must be able to do this without fear.

An inappropriate website is accessed unintentionally in academy by a teacher or child:

- Play the situation down, don't make it worse.
- Report to the DSL and decide whether to inform parents of any children who viewed the site.
- Inform the academy's network manager by logging the issue with Civica.

An inappropriate website is accessed intentionally by a child:

- Refer to the ICT policy (student guidance) and apply sanctions in line with the academy's behaviour policy.
- Report to a DSL who will inform the parents.
- Inform the academy's network manager by logging the incident with Civica.

An adult uses Academy IT equipment inappropriately:

- Where possible, ensure you have a colleague with you; do not view the misuse alone.
- Investigate the problem thoroughly and report any serious misuse immediately to the Principal and ensure that there is no further access to the PC or laptop. If the material is offensive but not illegal, the Principal should then:
    - Remove the PC to a secure place.

- Instigate an audit of all ICT equipment by the academy's ICT managed service providers to ensure there is no risk of pupils accessing inappropriate materials in the academy.
- Identify the precise details of the material.
- Take appropriate disciplinary action.
- Inform governors of the incident.

In an extreme case where the material is of an illegal nature:

- Remove the PC to a secure place.
- Document all action taken.
- Contact the appropriate authorities.

A bullying incident directed at a child occurs through email, website, messaging system or mobile phone technology and is in any way connected to the Academy:

- Advise the child not to respond to the message.
- Secure and preserve any evidence.
- Report to a DSL who will inform the service provider and notify parents of the children involved.
- Apply sanctions in line with the Academy's behaviour policy.
- Inform the Principal who will, depending on the severity of the incident consider informing the police and/or Birmingham LSCB.

Malicious or threatening comments are posted on an Internet site (e.g. blogs or social networking sites) about a pupil or member of staff:

- Inform and request the comments be removed if the site is administered externally.
- Secure and preserve any evidence.
- Investigate thoroughly and apply sanctions as appropriate.
- Inform the Principal who will, depending on the severity of the incident consider informing the police and/or Birmingham LSCB.

You are concerned that a child's safety is at risk because you suspect someone is using communication technologies (such as social networking sites, email or mobile devices) to make inappropriate contact with the child:

- Report to and discuss with the DSL in the Academy and contact parents.
- Advise the child on how to terminate the communication and save all evidence.
- Contact CEOP http://www.ceop.gov.uk
- Consider the involvement of police and social services.