PART OF THE PATHWAY ACADEMY TRUST

Meopham Community Academy

Enjoy, Learn, Aspire

Online Safety Policy

This policy was reviewed by: Tim Filewod, Computing Subject Leader
Date: May 2018
Approved by Governors: May 2018
Next Review Date: May 2020

Teaching and learning

Why is Internet use important?

- The Internet is a part of everyday life for education, business and social interaction. The Academy has a duty to provide children with quality Internet access as part of their learning experience.
- Internet use is part of the statutory curriculum and a necessary tool for learning.
- Pupils use the Internet widely outside the Academy and need to learn how to evaluate Internet information and to take care of their own safety and security.

How can Internet use enhance learning?

- The Academy's Internet access will be designed to enhance and extend education.
- Children will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- The Academy will ensure that the copying and subsequent use of Internet-derived materials by staff and children complies with copyright law.
- Access levels to the Internet will be reviewed to reflect the curriculum requirements and the age and ability of children.
- Children will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation. They will be encouraged to use google kids safe search. A shortcut is included on the academy website homepage.

How will children learn how to evaluate Internet content?

- Children will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Children will use age-appropriate tools to research Internet content.
- The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-Academy requirement across the curriculum.

Managing Information Systems

How will information systems security be maintained?

- The security of the Academy Information systems and users will be reviewed regularly.
- Virus protection will be updated regularly.
- The use of user logins and passwords to access the Academy network will be enforced.

How will email be managed?

- Children may only use approved email accounts for Academy purposes.
- Children must immediately tell a teacher if they receive offensive email.
- Children must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult.
- Whole class or group email addresses will be used for communication outside of the Academy.
- Staff will only use official Academy provided email accounts to communicate with children and parents/ carers, as approved by the senior management.
- Children will only send email to other recipients approved by members of the teaching staff.
- The forwarding of chain letters is not permitted.
- Staff should not use personal email accounts for professional purposes.

How will published content be managed?

- The contact details on the website should be the Academy address, email and telephone number. Staff or children's personal information must not be published.
- The Head Teacher will take overall editorial responsibility for online content published by the Academy and will ensure that content published is accurate and appropriate.

Can children's images or work be published?

- Images or videos that include children will be selected carefully and will not provide material that could be reused.
- Children's full names will not be used anywhere on the website, particularly in association with photographs.
- Written permission from parents or carers will be obtained before images/ videos of children are electronically published.
- Children's work can only be published with the permission of the parents.

How will social networking, social media and personal publishing be managed?

- The Academy will control access to social media and social networking sites.
- Staff wishing to use social media tools with children as part of the curriculum will risk assess the sites before use and check the sites terms and conditions to ensure the site is age appropriate. Staff will obtain documented consent from senior management before using social media tools in the classroom.
- Children will be advised never to give out personal details of any kind which may identify them and/ or their location. Examples would include real name, address, mobile or landline numbers, Academy attended, IM and email addresses, full names of friends/ family, specific interests and clubs etc.
- Children and parents will be advised that the use of social network spaces outside the Academy is inappropriate for primary aged pupils.
- Parents and visitors to the school will be advised verbally that any images recorded on their personal devices such as in the case of a class assembly, are strictly for personal use only. They are not to be published on social networking sites.
- All members of the Academy's community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.
- Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff professional behaviour.

How will filtering be managed?

- The Academy's broadband access will include filtering appropriate to the age and maturity of pupils.
- The Academy will work with Kent County Council and the Schools Broadband team to ensure that the filtering policy is continually reviewed.
- The Academy will have a clear procedure for reporting breaches of filtering. All members of the Academy's community (all staff and all pupils) will be aware of this procedure to report to the Deputy Head.
- The Academy's filtering system will block all sites on the Internet Watch Foundation (IWF) list.
- If staff or children discover an unsuitable site, it must be reported to the Online Safety Coordinator, who will then record the incident and escalate the concern as appropriate.

How will videoconferencing be managed?

- Children will ask permission from a teacher before making or answering a videoconference call.
- Videoconferencing will be supervised appropriately for the children's age and ability.
- Parents and carers consent should be obtained prior to children taking part in videoconferences.

How are emerging technologies managed?

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in the Academy is allowed.
- Mobile phones should not be brought into the Academy by the children, except in exceptional circumstances, when they should be handed into the Academy's office before the school day and collected at the end of the day.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulation (GDPR). The GDPR forms part of the data protection regime in the UK, together with the new Data Protection Act 2018 (DPA 2018). The main provisions of this apply, like the GDPR, from 25 May 2018.

Policy Decisions

How will Internet access be authorised?

- All staff will read and sign the 'Acceptable ICT Use Agreement' before using any Academy ICT resources.
- The Academy will keep a record of all staff and children who are granted access to the Academy's electronic communications.
- In Key Stage 1, children's access to the Internet will be by adult demonstration with occasional directly supervised access to specific and approved online materials.
- In Key Stage 2, children will be supervised. The children will use age-appropriate search engines and online tools and online activities will be teacher-directed where necessary.
- Parents will be asked to sign and return a consent form for the children's access and discuss it with their child, where appropriate.
- When considering access for vulnerable members of the Academy's community (such as with children with special education needs), the Academy will make decisions based on the specific needs and understanding of the child/children.

How will risks be assessed?

- The Academy will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that unsuitable material will never occur via an Academy computer. Neither the Academy nor Kent County Council can accept liability for the material accessed, or any consequences of Internet use.
- The Academy will audit Information Communication Technology use to establish if the Online Safety policy is adequate and that the implementation of the Online Safety policy is appropriate.

How will the Academy respond to any incidents of concern?

- All members of the Academy's community will be informed about the procedure for reporting Online Safety concerns (such as breaches of filtering, cyberbullying, illegal content etc).
- The Online Safety Coordinator will record all reported incidents and actions taken in the School Online Safety incident log.
- The designated Safeguarding Coordinator will be informed of any Online Safety incidents involving Safeguarding concerns, which will then be escalated appropriately.

How will Online Safety complaints be handled?

- Complaints about Internet misuse will be dealt with under the Academy's complaints procedure.
- Any complaint about staff misuse will be referred to the Head Teacher.
- All Online Safety complaints and incidents will be recorded by the Academy, including any actions taken.
- All members of the Academy's community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the Academy's community.

How is the internet used across the community?

- The Academy will liaise with local organisations to establish a common approach to Online Safety.
- The Academy will provide appropriate levels of supervision for students who use the Internet and technology whilst on the site.

How will cyberbullying be managed?

- Cyberbullying (along with all other forms of bullying) of any member of the Academy community will not be tolerated. Full details are set out in the Academy's policy on anti-bullying and behaviour.
- There are clear procedures in place to support anyone in the Academy's community affected by cyberbullying.
- All incidents of cyberbullying reported to the Academy will be recorded.
- There will be clear procedures in place to investigate incidents or allegations of cyberbullying.
- Children, staff and parents/ carers will be advised to keep a record of the bullying as evidence.
- The Academy will take steps to identify the bully, where possible and appropriate action taken.

How will Learning Platforms be managed?

- Senior management and staff will regularly monitor the usage of the Learning Platform by children and staff in all areas, in particular message and communication tools and publishing facilities.
- Children/ staff will be advised about acceptable conduct and use when using the Learning Platform.
- Only members of the current children, parents/ carers and staff community will have access to the Learning Platform.
- All users will be mindful of copyright issues and will only upload appropriate content onto the Learning Platform.
- When staff, children etc leave the Academy, their account or rights to specific Academy areas will be disabled or transferred to their new establishment.

How will mobile phones and personal devices be managed?

- The use of mobile phones and other personal devices by children and staff in the Academy will be decided by the Academy.
- Mobile phones should not be brought into the Academy by the children, except in exceptional circumstances, when they should be handed into the Academy's office before the school day and collected at the end of the day.
- Staff are not permitted to use their own personal phones or devices for contacting children and their families within or outside of the setting in a professional capacity.
- Staff should not use personal devices such as mobile phones or cameras to take photos or videos of children and will only use work provided equipment for this purpose.
- In accordance with the Early Years Statutory Framework, staff should not use mobile phones in areas of the Academy when children are present. Staff should therefore only use/ check mobiles in the staffroom during the academic day.

Communications Policy

How will the policy be introduced to children?

- All users will be informed that network and Internet use will be monitored.
- An Online Safety training programme will be established across the Academy to raise the awareness and importance of safe and responsible internet use amongst the children.
- Child instruction regarding responsible and safe use will precede Internet access.
- An Online Safety Scheme of Work will be included as part of the Computing curriculum.
- Online Safety rules will be posted in all rooms with Internet access.
- Particular attention to Online Safety education will be given where children are considered to be vulnerable.

How will the policy be discussed with staff?

- The Online Safety policy will be formally provided to and discussed with all members of staff.
- To protect all staff and children, the Academy will implement acceptable use policies.
- Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally will be provided for all members of staff.
- All members of staff will be made aware that their online conduct out of the Academy could have an impact on their role and reputation within the Academy.

How will parents' support be enlisted?

- Parents' attention will be drawn to the Academy Online Safety Policy in newsletters, the Academy prospectus and on the Academy Website.
- A partnership approach to Online Safety at home and at the Academy will be encouraged.
- Parents will be requested to sign an Online Safety/ Internet agreement as part of the home/ Academy agreement.
- Information and guidance for parents on Online Safety will be made available to parents in a variety of formats.
- Advice on useful resources and websites and filtering systems which include responsible use of the Internet will be made available to parents.
- Parents who help in lessons which involve using the Internet will be reminded to be Online Safety aware.

Inclusion and Equal opportunities

Delivery of this subject follows the Academy policy on Inclusion. Equal opportunities are given to all children, whatever their age, gender, ethnicity, attainment and background. The teaching and learning, achievements, attitudes and well being of every child matters, taking into account their varied life experiences and needs. We monitor the progress of each child through agreed assessment procedures.

We pay attention to the provision made for the different groups of children within the Academy:

- Girls and Boys
- Minority ethnic and faith groups, travellers, asylum seekers and refugees
- Children who need support to learn English as an additional language
- Children with additional educational needs
- Gifted and talented children
- Children 'looked after' by the local authority
- Other children, such as sick children; young carers; those from families under stress.
- Any children who are at risk of disaffection and exclusion

For children with additional educational needs

- Some children will lack the ability to regulate their own behaviour online and will require closer supervision and instruction.
- Online safety education will need to be repeated. One off events or assemblies will not be effective.
- Rules are very helpful to children and it is important to achieve consistency of how the rules are applied. It may be helpful to present them linked to consequences.
- The general Online Safety messages may need to be broken down and explained in greater detail in a variety of contexts and approaches.
- Children may require lots of examples of safe and unsafe experiences.
- Visual support is usually important to help most children to understand, but some areas of this topic are quite abstract in nature and difficult to represent visually, for example uncomfortable, smart, stranger, friend. It might be helpful to ask them to produce a drawing that defines these words.
- They are vulnerable to poor social understanding that may leave them open to risks when using the internet individually, but also when with peers.
- They may find it difficult to explain or describe events when using the internet and be unable to identify risks.
- They may not be able to ask for help or verbalise concerns. Adult supervision is a safe way to improve their recognition of this.

This provision is regularly considered and adapted accordingly. We promote the participation and the success of these groups of children and make sure that they are not disadvantaged within the Academy. We identify children who are underachieving or seem disengaged. We actively promote tolerance and understanding in a diverse society.

Children's individual needs will be addressed through provision of resources, learning styles and questioning and a positive use of technology will be promoted by all.

Internet Safety Contacts and References

- *CEOP (Child exploitation and Online Protection Centre) www.ceop.police.uk*
- *Online Safety Officer, Children's Safeguards Team, Families and Social Care, Kent County Council, esafetyofficer@kent.gov.uk*
- *Officer for Training and Development, Children's Safeguards Team, Families and Social Care, Kent County Council*
- *Children's Safeguards Team www.kelsi.org.uk/curriculum and pupil learning/early years and childcare/ safeguarding.aspx*
- *Click Clever Click Safe Campaign www.nidirect.gov.uk/click-clever-click-safe*
- *Cybermentors www.cybermentors.org.uk*
- *Digizen www.digizen.org.uk*
- *EIS Information Communication Technology support for schools www.eiskent.co.uk*
- *Internet Watch Foundation www.iwf.org.uk*
- *Kent Online Safety in Schools Guidance www.kelsi.org.uk*

- *Kent Police In an emergency (a life is in danger or a crime is in progress) dial 999. For other non-urgent enquiries contact the Safer Schools Partnership Officer www.kent.police.uk or www.kent.police.uk/internetsafety*
- *Kent Public Service Network www.kpsn.net*
- *Kent Safeguarding Children Board www.kscb.org.uk*
- *Kidsmart www.kidsmart.org.uk*
- *Schools Broadband Service Desk – Help with filtering and network security www.eiskent.co.uk*
- *Schools Online Safety Blog www.kenttrustweb.org.uk?esafetyblog*
- *Think U Know website www.thinkuknow.co.uk*
- *Virtual Global Taskforce – Report abuse www.virtualglobaltaskforce.com*