Abbey Hey E-Safety Policy 2017

Abbey Hey Primary Academy takes E-Safety very seriously and the following policies and procedures detail how we try to keep pupils safe in school:

- E-Safety Policy
- Acceptable Usage of Technology Policy
- Anti-Bullying Policy
- Teaching and Learning Policy
- Safeguarding

These policies are available through the school office and are available at : www.abbeyheyprimary.org.uk

Identified Risks

- We know that most of our pupils will use mobile devices and computers at some time. They are a source of fun, entertainment, communication and education. However, we know that some men, women and young people will use these technologies to harm children. The harm might range from sending hurtful or abusive texts and emails, to enticing children to engage in sexually harmful conversations, webcam photography or face-to-face meetings; or exposing them to harmful terrorist or extremist material.
- Cyberbullying by pupils, via texts, emails, mobile communication or social networking is treated as seriously as any other type of bullying and is managed through our anti-bullying procedures.
- Chatrooms and social networking sites are the more obvious sources of inappropriate and harmful behaviour and pupils are not allowed to access these sites on school owned devices.
- Some pupils will undoubtedly be 'chatting' on mobiles or social networking sites at home.

Key personal

The ICT Coordinator will have prime responsibility for updating the E-safety policy. The Senior Leadership Team and Governing Body will review twice a year. E-safety training will be delivered by both ICT Coordinator and Technology partner from UL.

- The school has appointed an e–Safety Coordinator.
- The e–Safety Policy and its implementation will be reviewed annually.
- Our e–Safety Policy has been written by the school, building government and UL guidance.
- Our School Policy has been agreed by the Senior Leadership Team and approved by governors.
- The School has appointed a member of the Governing Body to take lead responsibility for e-Safety.
- Our SENCO – Tracey Short

Filtering procedures at Abbey Hey Primary

The school's ICT is maintained by MGL and this group liaise with the SLT and ICT team to have an agreed filtering system. This includes possible radicalisation, risks to the well-being of the child either physical or mental, as well as indications of inappropriate behaviour (e.g. attempts to access pornography, in particular, extreme pornography).

The ICT team and SLT have a responsibility to monitor any unacceptable search terms, usage or e-safety concerns from any children or staff. This will be raised by a weekly report provided by MGL and will be checked by 2 members off staff each week.

Policy Statement

Communicating with children electronically

At Abbey Hey Primary Academy staff will only communicate with pupils face to face. They will not email children or use any of method of communication or social network. When using ipads, children will be able to communicate with staff via apps such as Showbie but this will be to discuss feedback and progress. Twitter should not be used between staff and pupils. Using online services and sites, not provided by United Learning, to communicate between a teacher and a student may put one or both participants at risk. This is because; it is not open and transparent, there is no audit trail, United Learning do not control the communication channel so cannot access the data, it is impossible to monitor (even when it takes place in school). The school's facebook page and twitter account will be monitored and administrated by Rachel Knock and Holly Brown. All messages which are due to go out will be emailed to these members of staff and they will be checked and added to the page.
Please refer to the social media policy for more guidance.

Education – students / pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating students / pupils to take a responsible approach. The education of students / pupils in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum. The e-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned e-safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited
- Key e-safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- Students / pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Students / pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
    - The ICT curriculum will include age appropriate lessons on e-safety including; keeping personal data safe, what children can do to stay safe online and how to report inappropriate material to the website owner.
- Students / pupils should be helped to understand the need for the student / pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff should act as good role models in their use of digital technologies the internet and mobile devices – which should be kept in a safe area (coat pockets in a cupboard which children have no access to) while the children are in school.
- In lessons where internet use is pre-planned, it is best practice that students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where students / pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Education – parents / carers

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- *Curriculum activities*
- *Letters, newsletters, web site*
- *Parents / Carers evenings / sessions*
- *High profile events / campaigns e.g. Safer Internet Day*
- *Reference to the relevant web sites / publications eg*

www.swgfl.org.uk www.saferinternet.org.uk/
http://www.childnet.com/parents-and-carers

Education – The Wider Community

The school / academy will provide opportunities for local community groups / members of the community to gain from the school's / academy's e-safety knowledge and experience. This may be offered through the following:

- *Providing family learning courses in use of new digital technologies, digital literacy and e-safety*
- *E-Safety messages targeted towards grandparents and other relatives as well as parents.*
- *The school / academy website will provide e-safety information for the wider community*
- *Supporting community groups e.g. Early Years Settings, Child-minders, youth / sports / voluntary groups to enhance their e-safety provision*
- *The school will offer advice and workshops for parents on keeping themselves, and their children, safe online*

Education & Training – Staff / Volunteers

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal e-safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the e-safety training needs of all staff will be carried out regularly. *It is expected that some staff will identify e-safety as a training need within the performance management process.*
- All new staff should receive e-safety training as part of their induction

programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Agreements.

- *The E-Safety Coordinator / Officer will receive regular updates through attendance at external training events (eg from SWGfL / LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations.*
- *This E-Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.*
- *The E-Safety Coordinator / Officer (or other nominated person) will provide advice / guidance / training to individuals as required.*

Complaints Procedure

How will the school respond to any incidents of concern?

- All members of the school community will be informed about the procedure for reporting e-Safety concerns (such as breaches of filtering, cyberbullying, illegal content etc).
- The e-Safety Coordinator/officer will record all reported incidents and actions taken in the School e-Safety incident log and other in any relevant areas e.g. Bullying or Child protection log.
- The Designated Child Protection Coordinator will be informed of any e-Safety incidents involving Child Protection concerns, which will then be escalated appropriately.
- The school will manage e-Safety incidents in accordance with the school discipline/ behaviour policy where appropriate.
- The school will inform parents/carers of any incidents of concerns as and when required.
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes required.

Schools e-Safety Audit

- This self-audit should be completed by the member of the Senior Leadership Team (SLT) responsible for e-safety policy. Staff that could contribute to the audit include: Designated Child Protection Coordinator, SENCO, e-Safety Coordinator, Network Manager and Head Teacher.

Has the school an e-Safety Policy that complies with UL guidance?	Y
The school e-safety policy was agreed by governors on: 2017	
The policy is available for staff to access at: www.abbeyheyprimary.org.uk	
The policy is available for parents/carers to access at: www.abbeyheyprimary.org.uk	
The responsible member of the Senior Leadership Team is: Tracey Short	
The governor responsible for e-Safety is: Catherine Horton-Hale	
The Designated Child Protection Coordinator is: Tracey Short	
The e-Safety Coordinator is: Holly Brown	
Were all stakeholders (e.g. pupils, staff and parents/carers) consulted with when updating the school e-Safety Policy?	Y
Has up-to-date e-safety training been provided for all members of staff? (not just teaching staff)	Y
Do all members of staff sign an Acceptable Use Policy on appointment?	Y
Are all staff made aware of the schools expectation around safe and professional online behaviour?	Y
Is there a clear procedure for staff, pupils and parents/carer to follow when responding to or reporting an e-Safety incident of concern?	Y
Have e-safety materials from CEOP, Childnet and UKCCIS etc. been obtained?	Y
Is e-Safety training provided for all pupils (appropriate to age and ability and across all Key Stages and curriculum areas)?	Y
Are e-safety rules displayed in all rooms where computers are used and expressed in a form that is accessible to all pupils?	Y

Do parents/carers or pupils sign an Acceptable Use Policy?	Y/N
Are staff, pupils, parents/carers and visitors aware that network and Internet use is closely monitored and individual usage can be traced?	Y
Is personal data collected, stored and used according to the principles of the Data Protection Act?	Y
Is Internet access provided by an approved educational Internet service provider which complies with DfE requirements (e.g. KPSN)?	Y
Has the school filtering been designed to reflect educational objectives and been approved by SLT?	Y
Are members of staff with responsibility for managing filtering, network access and monitoring systems adequately supervised by a member of SLT?	Y
Does the school log and record all e-Safety incidents, including any action taken?	Y
Are the Governing Body and SLT monitoring and evaluating the school e-Safety policy and ethos on a regular basis?	Y

E-Safety Contacts and References

UK Safer Internet Centre

- Safer Internet Centre -
- South West Grid for Learning
- Childnet
- Professionals Online Safety Helpline

- Internet Watch Foundation

CEOP

- http://ceop.police.uk/
- ThinkUKnow

Others:

- INSAFE - http://www.saferinternet.org/ww/en/pub/insafe/index.htm
- UK Council for Child Internet Safety (UKCCIS) www.education.gov.uk/ukccis
- Netsmartz http://www.netsmartz.org/index.aspx

Support for Schools

- Specialist help and support SWGfL BOOST

Cyberbullying

- Scottish Anti-Bullying Service, Respectme - http://www.respectme.org.uk/
- Scottish Government Better relationships, better learning, better behaviour
- DCSF - Cyberbullying guidance
- DfE – Preventing & Tackling Bullying – Advice to school leaders, staff and Governing Bodies
- Anti-Bullying Network - http://www.antibullying.net/cyberbullying1.htm
- Cyberbullying.org - http://www.cyberbullying.org/