ABBEYS PRIMARY SCHOOL

Aim, Aspire, Achieve @ Abbeys
Abbeys Primary School
Melrose Avenue
Bletchley
Milton Keynes
(01908) 375230

Website: www.abbeysprimaryschool.org
Email: abbeysprimary@milton-keynes.gov.uk

eSafety and Acceptable Use Policy

Date of policy: October 2020
Review Date: October 2021

Acceptable Use Policy

This policy has been developed with reference to schools' statutory responsibilities and takes account of national guidance and local procedures as follows:

- Keeping Children Safe in Education (2020)
  https://www.gov.uk/government/publications/keeping-children-safe-in-education--2

- Working together to safeguard children:
  https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/419595/Working_Together_to_Safeguard_Children.pdf

- Sexual violence and sexual harrassment between children in schools and colleges:
  https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/667862/Sexual_Harassment_and_Sexual_Violence_-_Advice.pdf

- Looked after Children Guidance (2018)
  https://www.gov.uk/government/publications/designated-teacher-for-looked-after-children

- Online Safety Guidance (2019)
  https://www.gov.uk/government/publications/teaching-online-safety-in-schools

At Abbeys Primary School we understand the responsibility to educate our pupils on eSafety issues; teaching them the appropriate behaviours and critical thinking 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.

Our designated eSafety leader is Miss Rebecca Fensom.

1. Rationale for an Acceptable Use and eSafety Policy

The statutory curriculum requires pupils to learn how to locate, retrieve and exchange information using computing. In delivering the curriculum, teachers need to plan to integrate the use of communications technology such as online resources and email. Computing skills are vital to access life-long learning and employment; computing is now considered as an essential life-skill and it is important we prepare the children for life in the digital world.

Most technologies present risks as well as benefits. Internet use for work, home, social and leisure activities is expanding in all areas of society. The use of the internet brings young people into a contact with a wide variety of influences, some of which may be unsuitable. It is therefore important that Abbeys adopts strategies for the safe and responsible use of computing.

It is important that teachers, parents and carers do not confuse skilful use of new technologies with an ability to perceive and avoid risk – internet and computer literacy is unfortunately not synonymous with internet and computer safety. *BECTA*

It is important not to take for granted that children who are proficient in their use of the internet, are also able to assess risk when dealing with new technology and e-learning. It is therefore the responsibility of Abbeys Primary School to ensure a safe e-learning environment for the children and the school as a whole. This policy aims to set out how this will be achieved.

2. Aims

To ensure the safeguarding of all children and young people within and beyond the school setting by detailing appropriate use of online technologies through clear rules, procedures and guidelines to minimise risks. These risks include:

- Being vulnerable to inappropriate contact from strangers
- Cyber-bullying
- Illegal activities of downloading or copying any copyright materials and file-sharing via the internet or mobile devices
- Issues with spam and other inappropriate email
- Online content which is abusive or offensive
- Use of social medial to encourage extremism
- Viruses

To outline the roles and responsibilities of all pupils, staff and parents/carers, ensuring all are clear about procedures for misuse of any online technologies both within and beyond the school setting.

To develop links with parents/carers and the wider community, ensuring their input into procedures with continued awareness of benefits and potential issues of online technologies.

3. Roles and responsibilities of the school

3.1 Governors, Head teacher and ICT subject leader.

It is the overall responsibility of the Headteacher and Computing subject leader with the Governors to ensure that there is an overview of eSafety (as part of the wider remit of Child Protection) across the school with further responsibilities as follows:

- The Headteacher has designated an eSafety Leader to implement agreed policies, procedures, staff training, curriculum requirements and take the lead responsibility for ensuring eSafety is addressed in order to establish a safe ICT learning environment.
- Time and resources will be provided for the eSafety Leader and staff to be trained and update policies, where appropriate. The Headteacher is responsible for promoting eSafety across the curriculum and has an awareness of how this is being developed, linked with the school development plan.
- The Governors must ensure Child Protection is covered with an awareness of eSafety and how it is being addressed within the school, as it is the

responsibility of Governors to ensure that all Child Protection guidance and practices are embedded.
- Ensure that any misuse or incident has been dealt with appropriately, according to policy and procedures and appropriate action is taken.

3.2 eSafety Leader

It is the role of the designated eSafety Leader with support from the Headteacher to:

- Ensure that the policy is reviewed annually, with up-to-date information available for all staff to teach eSafety and for parents to feel informed and know where to go for advice.
- Report issues and update the Headteacher on a regular basis.
- Liaise with the PSHE, Child Protection and Computing leads so that policies and procedures are up-to-date to take account of any emerging issues and technologies.
- Update staff training (all staff) according to new and emerging technologies so that the correct eSafety information can be taught or adhered to.
- Transparent monitoring of the Internet and online technologies – It is the class teacher's responsibility to monitor the use of the Internet and technologies by the children in their class.

3.3 Staff or adults

It is the responsibility of all adults within the school or other setting to:

- Ensure that they know who the Designated Safeguarding Lead is within school or other setting so that any misuse or incidents can be reported which involve a child. Where an allegation is made against a member of staff it should be reported immediately to the Headteacher. In the event of an allegation made against the Headteacher, the Chair of Governors must be informed immediately.
- Be familiar with the Behaviour, Anti-bullying and other relevant policies so that in the event of misuse or an allegation, the correct procedures can be followed, immediately.
- Alert the eSafety Leader of any new or arising issues and risks that may need to be included within policies and procedures.
- Ensure that children and young people are protected and supported in their use of online technologies so that they know how to use them in a safe and responsible manner so that they can be in control and know what to do in the event of an incident.
- Be up-to-date with eSafety knowledge that is age group appropriate and reinforce through the curriculum.
- Sign an Acceptable Use Statement to show that they agree with and accept the rules for staff using non-personal equipment, within and beyond the school environment, as outlined in appendices.
- Use electronic communications in an appropriate way that does not breach the Data Protection Act 1998.
  Remember confidentiality and not disclose information from the network, pass on security passwords or leave a station unattended when they or another user is logged in.

The School Business Manager will follow appropriate procedures for any data required to be taken from the school premises.

- Report accidental access to inappropriate materials to the e-Safety Leader in order that inappropriate sites are added to the restricted list.
- Use anti-virus software and check for viruses on their work laptop or memory stick when transferring information from the internet on a regular basis, especially when not connected to the school network.

3.4 Children and young people

Children and young people are:

- Consulted on Acceptable Use Rules through the school council or other appropriate group, in line with this policy being reviewed and updated.
- Taught to work online in a safe and responsible manner through Computing lessons as well as, PSHE or other clubs and groups.
- Taught to tell an adult about any inappropriate materials or contact from someone they do not know straight away, without reprimand.

4. Appropriate use

In the event that a child or young person **accidentally** accesses inappropriate materials the child will report this to an adult immediately and take appropriate action to hide the screen or close the window.

Children will be taught and encouraged to consider the implications for misusing the internet and posting inappropriate materials to websites, for example, as this can lead to legal implications.

5. The Curriculum and Tools for Learning

5.1 Internet use

We teach our children and young people how to use the internet safely and responsibly, for researching information, exploring concepts, deepening knowledge and understanding and communicating effectively in order to further learning, through Computing and/or PSHE lessons where the following concepts, skills and competencies have been taught by the time they leave Year 6 :

- Internet literacy
- making good judgements about websites and e-mails received
- knowledge of risks such as viruses and opening mail from a stranger
- access to resources that outline how to be safe and responsible when using any online technologies
- knowledge of copyright and plagiarism issues
- file-sharing and downloading illegal content
- uploading information – know what is safe to upload and not upload personal information
- where to go for advice and how to report abuse

Personal safety – ensuring information uploaded to web sites and e-mailed to other people does not include any personal information including:

- full name (first name is acceptable, without a photograph)
- address
- telephone number
- e-mail address

- school
- clubs attended and where
- age or DOB
- names of parents
- routes to and from school
- identifying information, e.g. I am number 8 in the Abbeys Football Team

5.2 Videos and digital images
Taking images via a web cam or other mobile device will follow the same procedures as taking images with a digital or video camera.

5.3 Mobile phones and other technologies
The use of mobile phones or mobile devices will not be allowed to be used in our school, or on school grounds if a child is attending an after-school club, or on a trip or residential visit.

Staff members are not allowed to use their personal numbers to contact children and young people under any circumstances.

5.4 Video and photographs
The term 'image' refers to the taking of video footage or photographs via any camera or other technology. When in school there is access to:

- digital cameras
- visualisers
- Learnpads
- iPads
- Web cams
- Photographs/images used to identify children and young people in a forum will be representative of the child rather than of the child e.g. an avatar.

Any photographs or video clips uploaded will not have a file name of a child, especially where these may be uploaded to a school website.

Photographs should only ever include the child's first name (although Child Protection Guidance states either a child's name or a photograph but not both.) If it is possible we prefer to have Group photographs rather than pictures of individual children.

6. Filtering and safeguarding measures
School internet access is controlled through the LA's broadband provider and checked by teachers in advance. The school is also able to block additional sites using the software on the schools Cachepilot.

Raw image searches are discouraged when working with pupils.

If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these

sites and supervise this work. Parents will be advised to supervise any further research.

Anti-virus and anti-spyware software is used on all network and stand alone PCs or laptops and is updated on a regular basis.

The wireless network has an Encryption code which will help prevent hacking.

7. Parents

7.1 Roles

Each child or young person receives a copy of the Acceptable Use Rules on first-time entry to the school which need to be read with the parent/carer, signed and returned to school confirming both an understanding and acceptance of the rules. When moving into Year 3 the children will receive a copy of the KS2 rules to be read with the parent/carer and signed as above.

It is expected that parents/carers will explain and discuss the rules with their child, where appropriate, so that they are clearly understood and accepted.

The school will keep a record of the signed forms.

Whilst we endeavour to safeguard and mitigate against all risks, we will never be able to eliminate them all completely. Any incidents that may come to our notice will be dealt with quickly and according to the school's policies to ensure the school continues to protect pupils.

October 2019

Appendices

Staff Procedures Following Misuse by Staff

The Headteacher will ensure that these procedures are followed, in the event of any misuse of the Internet, by an adult:

A. An inappropriate website is accessed inadvertently:
Report website to the eSafety Leader if this is deemed necessary.
Contact the ICT Network Support Consultant so that it can be added to the banned or restricted list.

B. An inappropriate website is accessed deliberately:
Ensure that no one else can access the material by shutting down.
Log the incident.
Report to the Headteacher and eSafety Leader immediately.
Headteacher to refer back to the Acceptable Use Rules and follow agreed actions for discipline.
Inform the ICT Network Support Consultant as with A.

C. An adult has communicated with a child or used ICT equipment inappropriately:
Ensure the child is reassured and remove them from the situation immediately, if necessary.
Report to the Headteacher and Designated Person for Child Protection immediately.
Preserve the information received by the child if possible and determine whether the information received is abusive, threatening or innocent.
Once Procedures and Policy have been followed and the incident is considered innocent, refer to the Acceptable Use Rules for Staff and Headteacher to implement appropriate sanctions.
If illegal or inappropriate misuse is known, contact the Headteacher or Chair of Governors (if allegation is made against the Headteacher) and Designated Person for Child Protection immediately and follow the Allegations procedure and Child Protection Policy.
Contact CEOP (police) as necessary.

D. Threatening or malicious comments are posted to a website (or printed out) about an adult in school:
Preserve any evidence.
Inform the Headteacher immediately and follow Child Protection Policy as necessary. Contact the police or CEOP as necessary.

E. Where staff or adults are posted on inappropriate websites or have inappropriate information about them posted, this should be reported to the Headteacher.

Staff Procedures Following Misuse by Children and Young People

The Headteacher will ensure that these procedures are followed, in the event of any misuse of the Internet, by a child or young person:

A. An inappropriate website is accessed inadvertently:
Reassure the child that they are not to blame and praise for being safe and responsible by telling an adult.
Report website to the eSafety Leader if this is deemed necessary.
Contact the IT Network Support Consultant.

B. An inappropriate website is accessed deliberately:
Refer the child to the Acceptable Use Rules that were agreed.
Reinforce the knowledge that it is illegal to access certain images and police can be informed.
Decide on appropriate sanction.
Notify the parent/carer.
Inform IT Network Support Consultant as above.

C. An adult or child has communicated with a child or used ICT equipment inappropriately:
Ensure the child is reassured and remove them from the situation immediately.
Report to the Headteacher and Designated Person for Child Protection immediately.
Preserve the information received by the child if possible and determine whether the information received is abusive, threatening or innocent.

D. Threatening or malicious comments are posted on external websites about an adult in the school or setting:
Preserve any evidence.
Inform the Headteacher immediately.

CEOP advice is to turn off the screen, secure the machine and contact the police for further instructions if an indecent image is found. They will advise on how to deal with the machine, if they are unable to send out a forensics team immediately. If in doubt, do not power down the machine.

Any offensive images that may be received should never be forwarded to anyone else, even if it is to report them as illegal as this constitutes illegal activity and you will be liable to prosecution and investigation by the police.

Acceptable Use Rules for Staff

These rules apply to all online use and to anything that may be downloaded or printed.

To ensure that all adults within the school setting are aware of their responsibilities when using any online technologies, such as the Internet or email, they are asked to sign these Acceptable Use Rules. This is so that they provide an example to children and young people for the safe and responsible use of online technologies which will educate, inform and protect and so that they feel safeguarded from any potential allegations or inadvertent misuse themselves.

- I know that I should only use the school equipment in an appropriate manner and for professional uses.
- I understand that I need to give permission to children and young people before they can upload images (video or photographs) to the internet.
- I know that images should not be inappropriate or reveal any personal information of children and young people if uploading to the Internet.
- I have read the Procedures for Incidents of Misuse so that I can deal with any problems that may arise, effectively.
- I will report accidental misuse.
- I will report any incidents of concern for children's or young people's safety to the Headteacher, Designated Person for Child Protection or eSafety Leader in accordance with procedures listed in the Acceptable Use and eSafety Policy.
- I know who my Designated Person for Child Protection is.
- I know that I am putting myself at risk of misinterpretation and allegation should I contact children and young people via personal technologies, including my personal email and should use the school email and phones. I know that I should not be using the school system for personal use unless this has been agreed by the Headteacher and/or eSafety Leader.
- I know that I should complete virus checks on my laptop and memory stick or other devices so that I do not inadvertently transfer viruses, especially where I have downloaded resources.
- I will only install hardware and software I have been given permission for.
- I will ensure that I follow the Data Protection Act 1998 and have checked I know what this involves.
- I will ensure that I keep my password secure and not disclose any security information unless to appropriate personnel. If I feel someone inappropriate requests my password I will check with the e-Safety Leader.
- I have been given a copy of the Acceptable Use Policy to refer to about all e-safety issues and procedures that I should follow.
- I will adhere to copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.

I have read, understood and agree with these Rules as I know that by following them I have a better understanding of eSafety and my responsibilities to safeguard children and young people when using online technologies.

Signed…….Date…….

Name (printed)……..

eSafety Acceptable Use Rules Letter to Parents/Carers

Dear Parent/Carer,

Computing - including use of the internet, email and mobile technologies, is an integral part of learning in our school. We expect all children to be safe and responsible when using any ICT.
Please read and discuss these eSafety rules with your child and return the slip at the bottom of this page.

These Rules provide an opportunity for further conversations between you and your child/young person about safe and appropriate use of the internet and digital devices, both within and beyond school .

Should you wish to discuss the matter further please contact the Headteacher.

Yours faithfully,

eSafety Leader

Child Agreement:

Name: _____Class:_____

- I understand the Rules for using the internet and digital devices, safely and responsibly.
- I know that the adults working with me at school will help me to stay safe and check that I am using the computers to help me with my work.

Child Signature: _____ Date: _____

Parent/Carer Agreement:

- I have read and discussed the Rules with my child and confirm that he/she has understood what the Rules mean.
- I understand that the school will use appropriate filtering and ensure appropriate supervision when using the Internet and online tools. I understand that occasionally, inappropriate materials may be accessed and accept that the school will endeavour to deal with any incident that may arise, according to policy.
- I understand that whilst my child is using the internet and other digital devices outside of school, that it is my responsibility to ensure safe and responsible use with the support of the school.

Parent/Carer Signature: _____ Date: _____

Key Stage 1

These are our rules for using the Internet safely.

Our Internet Rules

- We use the internet safely to help us learn.
- We learn how to use the internet.
- We can send and open messages with an adult.
- We can write polite and friendly messages to people that we know.
- We only tell people our first name, or we use a username.
- We know that we should not share our password or other personal information.
- We know who to ask for help.
- If we see something we do not like we know what to do.
- We know that it is important to follow the rules.
- We can go to www.thinkuknow.co.uk for help.

Key Stage 2

These are our rules for using the Internet safely and responsibly.

Our Internet Rules

- We use the internet to help us learn and we will learn how to use the internet safely and responsibly.
- We send messages that are polite and friendly.
- We will only message, chat to or video-conference people an adult has approved.
- Adults are aware when we use online tools, such as video-conferencing.
- We never give out passwords or personal information (like our surname, address or phone number).
- We never post photographs or video clips without permission and never include names with photographs.
- If we need help we know who to ask.
- If we see anything on the internet or in a message that makes us uncomfortable, we know what to do.
- If we receive a message sent by someone we don't know, we know what to do.
- We know we should follow the rules as part of the agreement with our parent/carer.
- We are able to look after each other by using the internet in a responsible way.
- We know that we can go to www.thinkuknow.co.uk for help.

Further Information and Guidance

The nature of e-safety is evolving, you may want to keep up to date with further supporting documents, information or advice, which can be found on:

- www.bbc.co.uk/onlinesafety (advice and links for children, teachers and parents/carers)
- www.bullying.co.uk (Online help and advice service combating all forms of bullying. Advice for children, parents/carers and schools.)
- www.bbc.co.uk/cbbc/help
- www.ceop.co.uk (for parents/carers and adults)
- www.thinkuknow.co.uk (for all children and young people with a section for parents/carers and adults – this also links with the CEOP (Child Exploitation and Online Protection Centre work)
- www.teachernet.gov.uk (for schools and settings)
- www.dcsf.gov.uk (for adults)
- www.childnet.com
- www.getsafeonline.org