CHURCH OF ENGLAND ACADEMY

Abbey GRANGE

Part of Abbey Multi Academy Trust

Policies and Procedures

eSafety Policy

eSafety Policy

Safeguarding students, staff and school in a digital world

Contents

Introduction

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- E-mail, Instant Messaging and chat rooms
- Social Media, including Facebook and Twitter
- Mobile/ Smart phones with text, video and/ or web functionality
- Making /receiving phone calls via their mobile phones
- Other mobile devices with web functionality
- Gaming, especially online
- Learning Platforms and Virtual Learning Environments
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading

This eSafety policy recognises the commitment of our school to eSafety and acknowledges its part in the school's overall Safeguarding policies and procedures. It shows our commitment to meeting the requirement to keep pupils safe when using technology. We believe the whole school community can benefit from the opportunities provided by the Internet and other technologies used in everyday life. The eSafety policy supports this by identifying the risks and the steps we are taking to avoid them. It shows our commitment to developing a set of safe and responsible behaviours that will enable us to reduce the risks whilst continuing to benefit from the opportunities.

The person in school taking on the role of eSafety lead is Rebecca Robinson

The Governor with an overview of eSafety matters is <<name>>

This eSafety policy was created by Rebecca Robinson

The following groups formed a working party and were consulted during the creation of this eSafety policy:

ESafety lead / ICT Teacher / Head of ICT Services / ICT Technician (Web/VLE) / Working party of Students (Anti-bullying ambassadors) / Assistant head teachers

The policy was completed on: November 2013

The policy was approved by Governing Body, December 2013

The policy is due for review no later than: December 2014

Implementation of the Policy

- The Senior Leadership Team (SLT) will ensure all members of school staff are aware of the contents of the school eSafety policy and the use of any new technology within school.
- All staff, students, occasional and external users of our school ICT equipment will be able to view the Acceptable Use Policy via the school website and by using the school systems are agreeing to its terms.
- ESafety will be taught as part of the curriculum in an age-appropriate way to all pupils.
- The eSafety policy will be made available to parents, carers and others via the school website.

Responsibilities of the School Community

We believe that eSafety is the responsibility of the whole school community and that everyone has their part to play in ensuring all members of the community are able to benefit from the opportunities that technology provides for learning and teaching. The following responsibilities demonstrate how each member of the community will contribute.

The Senior Leadership Team accepts the following responsibilities:

- The Principal will take ultimate responsibility for the eSafety of the school community
- Identify a person (the eSafety lead) to take day to day responsibility for eSafety; provide them with training and support them in their work.
- Ensure adequate technical support is in place to maintain a secure ICT system
- Ensure liaison with the Governors
- Develop and promote an eSafety culture within the school community
- Ensure that all staff, pupils and other users agree to the Acceptable Use Policy and that new staff have eSafety included as part of their induction procedures
- Receive and regularly review eSafety incident logs; ensure that the correct procedures are followed should an eSafety incident occur in school and review incidents to see if further action is required

Responsibilities of the eSafety Lead

- Promote an awareness and commitment to eSafety throughout the school
- Be the first point of contact in school on all eSafety matters
- Take day to day responsibility for eSafety within the school
- liaise with technical staff on eSafety issues
- Create and maintain eSafety policies and procedures
- Develop an understanding of current eSafety issues, guidance and appropriate legislation
- Ensure delivery of an appropriate level of training in eSafety issues
- Ensure that eSafety is promoted to parents and carers
- Monitor and report on eSafety issues to the eSafety group, the Leadership team and the Safeguarding/eSafety Governor as appropriate
- Ensure that staff and pupils know the procedure to follow should they encounter any material or communication that makes them feel uncomfortable and how to report an eSafety incident
- Ensure an eSafety incident log is kept up-to-date
- To promote the positive use of modern technologies and the internet

- To ensure that the school eSafety policy is reviewed

Responsibilities of all Staff

- Read, understand and help promote the school's eSafety policies and guidance
- Take responsibility for ensuring the safety of sensitive school data and information
- Develop and maintain an awareness of current eSafety issues, legislation and guidance relevant to their work
- Maintain a professional level of conduct in their personal use of technology at all times
- Ensure that all digital communication with pupils is on a professional level and only through school based systems, **NEVER** through personal email, text, mobile phone social network or other online medium.
- Embed eSafety messages in learning activities where appropriate
- Supervise pupils carefully when engaged in learning activities involving technology
- Ensure that pupils are told what to do should they encounter any material or receive a communication which makes them feel uncomfortable
- Report all eSafety incidents which occur in the appropriate log and/or to their line manager

Additional Responsibilities of Technical Staff

- Support the school in providing a safe technical infrastructure to support learning and teaching
- Ensure appropriate technical steps are in place to safeguard the security of the school ICT system, sensitive data and information. Review these regularly to ensure they are up to date
- Ensure that provision exists for misuse detection and malicious attack
- Report any eSafety-related issues that come to their attention to the eSafety lead and/or Senior Leadership Team
- Ensure that procedures are in place for new starters and leavers to be correctly added to and removed from all relevant electronic systems, including password management
- Ensure that suitable access arrangements are in place for any external users of the schools ICT equipment.
- Ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster.

Responsibilities of Students

- Take responsibility for their own and each other's' safe and responsible use of technology wherever it is being used, including judging the risks posed by the personal technology owned and used by them outside of school
- Ensure they respect the feelings of other students
- Ensure they respect the rights of other students
- Ensure they respect the values of others in their use of technology in school and at home

- Understand what action should be taken if they feel worried, uncomfortable, vulnerable or at risk whilst using technology, or if they know of someone to whom this is happening
- Report all eSafety incidents to appropriate members of staff
- Discuss eSafety issues with family and friends in an open and honest way
- To know, understand and follow school policies on the use of mobile phones, digital cameras and handheld devices
- To know, understand and follow school policies regarding bullying
- Students will support the school approach to online safety and not deliberately post comments or upload any images, sounds or text that could upset or offend any member of the school community or bring the school into disrepute.

Responsibilities of Parents and Carers

- Help and support the school in promoting eSafety
- Discuss eSafety concerns with their children, show an interest in how they are using technology, and encourage them to behave safely and responsibly when using technology
- Consult with the school if they have any concerns about their child's use of technology
- To agree to and sign the home-school agreement containing a statement regarding their personal use of social networks in relation to the school
- Parents and carers will support the school approach to online safety and not deliberately post comments or upload any images, sounds or text that could upset or offend any member of the school community or bring the school into disrepute
- To report any concerns via the Academies' website at www.abbeygrangeacademy.co.uk

Responsibilities of Governing Body

- Read, understand, contribute to and help promote the school's eSafety policies and guidance as part of the school's overarching Safeguarding procedures
- Support the work of the school in promoting and ensuring safe and responsible use of technology in and out of school, including encouraging parents to become engaged in eSafety awareness
- To have an overview of how the school IT infrastructure provides safe access to the internet and the steps the school takes to protect personal and sensitive data
- Ensure appropriate funding and resources are available for the school to implement their eSafety strategy

Responsibilities of the Child Protection Officer

- Understand and raise awareness of the issues and risks surrounding the sharing of personal or sensitive information
- Be aware of and understand the risks to young people from online activities such as grooming for sexual exploitation, sexting, cyber bullying and others.

Raise awareness of the particular issues which may arise for vulnerable pupils in the school's approach to eSafety ensuring that staff know the correct child protection procedures to follow.

Access to School Systems

The school decides which users should and should not have Internet access, the appropriate level of access and the level of supervision they should receive. There are robust systems in place for managing network accounts and passwords, including safeguarding administrator passwords. Suitable arrangements are in place for visitors to the school who may be granted a temporary log in.

All users are provided with a log in appropriate to their key stage or role in school. Pupils are taught about safe practice in the use of their log in and passwords.

Staff are given appropriate guidance on managing access to laptops which are used both at home and school and in creating secure passwords.

Access to personal, private or sensitive information and data is restricted to authorized users only, with proper procedures being followed for authorizing and protecting login and password information.

Passwords

- We ensure that a secure and robust username and password convention exists for all system access (email, network access, school management information system).
- We provide all staff with a unique, individually-named user account and password for access to IT equipment, email and information systems available within school.
- All pupils have a unique, individually-named user account and password for access to IT equipment and information systems available within school.
- All staff and pupils have responsibility for the security of their usernames and passwords and are informed that they must not allow other users to access the systems using their log on details. They must immediately report any suspicion or evidence that there has been a breach of security.
- The school maintains a log of all accesses by users and of their activities while using the system in order to track any eSafety incidents.
- Password must be difficult to guess and should be a mixture of upper case and lowercase, numbers and symbols.
- Students will have to reset their passwords at given intervals.

Securus

We use a system within the school called secures for monitoring PC activity. Securus runs in the background of all PC's scanning for certain, word and phrases and other such items as pictures with a certain percentage of flesh tones. When Securus picks up a hit it takes a screenshot as a violation. Violations are monitored by a combination of the schools Safer Partnership Officer and ICT administrators. Appropriate action is taken depending on the violation.

Using the Internet

We provide the internet to:

- Support curriculum development in all subjects
- Support the professional work of staff as an essential professional tool
- Enhance the school's management information and business administration systems
- Enable electronic communication and the exchange of curriculum and administration data with the examination boards and others

Users are made aware that they must take responsibility for their use of, and their behaviour whilst using the school IT systems or a school provided laptop or device and that such activity can be monitored and checked.

Using Email

Email is regarded as an essential means of communication and the school provides all members of the school community with an e-mail account for school based communication. Communication by email between staff, pupils and parents will only be made using the school email account and should be professional and related to school matters only. E-mail messages on school business should be regarded as having been sent on headed notepaper and reflect a suitable tone and content and should ensure that the good name of the school is maintained.

All email activity is recorded in line with data protection laws. The school is able to view these records in situations where this is called upon.

It is the personal responsibility of the email account holder to keep their password secure.

As part of the curriculum pupils are taught about safe and appropriate use of email. Pupils are informed that misuse of email will result in a loss of privileges.

School will set clear guidelines about when pupil-staff communication via email is acceptable and staff will set clear boundaries for pupils.

Under no circumstances will staff contact pupils, parents or conduct any school business using a personal email addresses.

Responsible use of personal web mail accounts on school systems is permitted for staff only outside teaching hours.

Receiving Emails

- Check your e-mail regularly
- Activate your 'out-of-office' notification when away for extended periods
- Never open attachments from an untrusted source

Publishing content online

E.g. using the school website, Learning Platform, blogs, social network sites

School Website:

The school maintains editorial responsibility for any school initiated web site or publishing online to ensure that the content is accurate and the quality of presentation is maintained. The school maintains the integrity of the school website by ensuring that responsibility for uploading material is always moderated and that passwords are protected.

The point of contact on the web site is the school address, e-mail and telephone number.

Identities of pupils are protected at all times. Parents have the option to opt out so that photographs of individual pupils are not published on the website. Group photographs do not have a name list attached.

Online Material Published Outside the School:

Staff and pupils are encouraged to adopt similar safe and responsible behaviours in their personal use of blogs, wikis, social networking sites and other online publishing outside school as they are in school.

Material published by pupils, governors and staff in a social context which is considered to bring the school into disrepute or considered harmful to, or harassment of another pupil or member of the school community will be considered a breach of school discipline and treated accordingly.

Using Images, Video and Sound

We recognize that many aspects of the curriculum can be enhanced by the use of multi-media and that there are now a wide and growing range of devices on which this can be accomplished. Pupils are taught safe and responsible behaviour when creating, using and storing digital images, video and sound.

Digital images, video and sound recordings are only taken with the permission of participants and their parents; images and video are of appropriate activities and are only taken of pupils wearing appropriate dress.

We ask all parents/carers to opt out if they do not want photographs and video of their children (in publications and on websites).

For their own protection staff or other visitors to school never use a personal device (mobile phone, digital camera or digital video recorder) to take photographs of pupils.

We are happy for parents to take photographs at school events but will always make them aware that they are for personal use only and if they have taken photographs of children other than their own they should not be uploaded to social media sites and can be only used for their personal use.

Using Other Technologies

As a school we will keep abreast of new technologies and evaluate both the benefits for learning and teaching and also the risks from an eSafety point of view.

We will regularly review the eSafety policy to reflect any new technology that we use, or to reflect the use of new technology by pupils.

Staff or pupils using a technology not specifically mentioned in this policy, or a personal device whether connected to the school network or not, will be expected to adhere to similar standards of behaviour to those outlined in this document.

Dealing with eSafety Incidents

All eSafety incidents are recorded in the School Behaviour Management System.

In situations where a member of staff is made aware of a serious eSafety incident, concerning pupils or staff, they will inform the eSafety Lead, child protection officer, their line manager or principal who will then respond in the most appropriate manner.

Instances of cyberbullying will be taken very seriously by the school and dealt with using the schools anti-bullying procedures. School recognizes that staff as well as pupils may be victims and will take appropriate action in either situation, including instigating restorative practices to support the victim.

Incidents which create a risk to the security of the school network, or create an information security risk, will be referred to the school's eSafety Lead and technical support and appropriate advice sought and action taken to minimize the risk and prevent further instances occurring, including reviewing any policies, procedures or guidance. If the action breaches school policy then appropriate sanctions will be applied. The school will decide if parents need to be informed if there is a risk that pupil data has been lost.

School reserves the right to monitor equipment on their premises and to search any technology equipment, including personal equipment with permission, when a breach of this policy is suspected.

Dealing with Complaints and Breaches of Conduct by Pupils:

- Any complaints or breaches of conduct will be dealt with promptly
- Responsibility for handling serious incidents will be given to a senior member of staff
- Parents and the pupil will work in partnership with staff to resolve any issues arising
- Restorative practice will be used to support the victims
- There may be occasions when the police must be contacted. Early contact will be made to establish the legal position and discuss strategies

The following activities constitute behaviour which we would always consider unacceptable (and possible illegal):

- accessing inappropriate or illegal content deliberately
- deliberately accessing downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- continuing to send or post material regarded as harassment, or of a bullying nature after being warned
- staff using digital communications to communicate with pupils in an inappropriate manner (for instance, using personal email accounts, personal mobile phones, or inappropriate communication via social networking sites)
- The following activities would normally be unacceptable; in some circumstances they may be allowed e.g. as part of planned curriculum activity or by a system administrator to problem solve
- accessing social networking sites, chat sites, instant messaging accounts, email or using a mobile phone for personal use during lesson time
- accessing non-educational websites (e.g. gaming or shopping websites) during lesson time
- sharing a username and password with others or allowing another person to log in using your account
- accessing school ICT systems with someone else's username and password
- deliberately opening, altering, deleting or otherwise accessing files or data belonging to someone else

Schedule of Development / Monitoring / Review of the Policy

	Date
The implementation of this e-safety policy will be monitored by the:	
Monitoring will take place at regular intervals:	
The eSafety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place.	
Should serious e-safety incidents take place, the following internal / external persons / agencies should be informed:	Principal / Senior Safeguarding Officer / Designated esafety lead / Safer Schools Officer

The school will monitor the impact of the policy using:

- Logs of reported incidents on the BMS
- Monitoring logs of internet activity (including sites visited)
- Internal monitoring data for network activity