

| | |
|-------------------------|--|
| Agreed by | |
| SMT/BOG | |
| REVIEW DATE | |
| Person/s Responsible | |

E Safety Policy



Abbey Primary School

Contents

Introduction

Roles and Responsibilities

Teaching and Learning

Use of Digital and Video Images

Use of email and School Website

Use of Internet

Use of Mobile Phones

Monitoring and Filtering

Procedures should incidents occur

Cyberbullying

Data Protection

Communication of Policy to Pupils, Staff and Parents

Monitoring and Evaluation of the e-Safety Policy

This policy forms part of the school development plan and relates to other school policies including those for ICT, Anti-Bullying and Child Protection. The policy has been written by the school based on guidance material from The Department of Education and it has been approved by the Board of Governors. The Vice Principals is the e-Safety Co-ordinator and is the main point of contact for any issues relating to ICT in the context of child protection.

Introduction: The Need for an e-Safety Policy

In today's society, children, young people and adults interact with technologies such as mobile phones, games consoles and the internet on a daily basis and experience a wide range of opportunities, attitudes and situations. The exchange of ideas, social interaction and learning opportunities involved are greatly beneficial to all, but can occasionally place children, young people and adults in danger.

e-Safety covers issues relating to children and young people as well as adults and their safe use of the internet, mobile phones and other electronic communications technologies, both in and out of school. It includes education for all members of the school community on risks and responsibilities and is part of the "duty of care" which applies to everyone working with children.

Children should be empowered and educated so that they are equipped with the skills to make safe and responsible decisions as well as to feel able to report any concerns. All members of staff need to be aware of the importance of good e-Safety practice in the classroom in order to educate and protect the children in their care. Members of staff also need to be informed about how to manage their own professional reputation online and demonstrate appropriate online behaviours compatible with their role.

Abbey Primary School's e-Safety policy will demonstrate how the school plans to develop and establish its e-Safety approach and will identify core principles which all members of the school community need to be aware of and understand.

Roles and Responsibilities

The following section outlines the e-Safety roles and responsibilities of individuals and groups within the school.

Governors

Governors are responsible for the approval of the e-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors, receiving regular information about e-Safety incidents and monitoring reports.

Principal

- The Principal has a duty of care for ensuring the safety (including e-Safety) of members of the school community.
- The Principal and Vice Principal should be aware of the procedures to be followed in the event of a serious e-Safety allegation being made against a member of staff.
- The Senior Management Team will receive regular updates from the e-Safety Co-ordinator.

e-Safety Co-ordinator

The role of the school's designated e-Safety Co-ordinator will include e-Safety as per the 360° Internet Safety Audit Guidelines. The e-Safety Co-ordinator will:

- take day to day responsibility for e-Safety issues and incidents
- liaise and report regularly with Governors, SMT, ICT Co-ordinators and staff on e-Safety matters
- have a leading role in reviewing the school's e-Safety policies
- ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place
- provide training and advice for staff
- liaise with external bodies (e.g. SEELB, PSNI, Social Services etc.)
- receive reports of e-Safety incidents and create a log of incidents to inform future e-Safety developments
- attend relevant training
- be aware of the potential of serious child protection /safeguarding issues arising from, sharing of personal data, access to illegal/inappropriate materials, inappropriate on-line contact with adults/strangers, potential or actual incidents of grooming and cyberbullying.
- Highlight e-safety strategies to pupils in assemblies on a regular basis.

Teaching and Support Staff

Teaching and Support Staff are responsible for ensuring that:

- they have an up to date awareness of the school's e-Safety Policy
- they have read, understood and signed the Staff Acceptable Use Policy (AUP)
- they report any suspected misuse or problem to the Principal
- e-Safety issues are embedded in all aspects of the curriculum and other activities
- they implement current policies with regard to ICT devices
- they follow the appropriate procedures if any unsuitable material is found during internet searches
- pupils understand and follow the e-Safety and Acceptable Use Policies
- pupils avoid plagiarism and uphold copyright regulations
- pupils are guided to pre-planned, checked internet sites during lessons, where appropriate and under the direction of the class teacher

Pupils

At all times, pupils are expected to use ICT devices responsibly and follow the Pupil Acceptable Use Policy.

They should:

- avoid plagiarism and uphold copyright regulations
- immediately report to a member of staff any abuse, misuse or access to inappropriate materials
- be aware of the acceptable levels of behaviour relating to ICT devices
- be aware of the acceptable levels of behaviour relating to taking or using images
- be aware of the acceptable levels of behaviour relating to cyberbullying
- understand the importance of adopting good e-Safety practice when using digital technologies out of school and realize that the school's e-Safety Policy covers their actions out of school, if related to their membership of the school.

Parents/Carers

Parents/Carers play a crucial role in ensuring that their children understand the need to use the Internet/ICT devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website/Virtual Learning Environment and information about e-Safety campaigns and literature. Parents and carers will be encouraged to support the school in promoting good e-Safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- their children's personal devices, in school/on trips, where permitted

Teaching and Learning

The rapid developments in electronic communications are having many effects on society. The Internet is a part of everyday life for education, business and social interaction. Internet use is part of the statutory curriculum and is a necessary tool for learning. The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions. Pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security. The school therefore has a duty to provide pupils with quality Internet access as part of their learning experience.

There are many educational benefits to be gained through the appropriate use of the Internet. There is immediate access to:

- learning wherever and whenever convenient
- worldwide educational resources, such as museums and art galleries
- educational and cultural exchanges between pupils worldwide
- vocational, social and leisure use in libraries, clubs and at home
- experts in many fields for pupils and staff
- professional development for staff through access to national developments, educational materials and effective classroom practice
- vocational, social and leisure use in libraries, clubs and at home

The school's internet access will be designed to enhance and extend education. Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use. Abbey Primary School will ensure that the copying and subsequent use of Internet-derived materials by staff and pupils complies with copyright law. Access levels to the internet will be reviewed regularly to ensure that they reflect the curriculum requirements, age and ability of the pupils. Staff will guide pupils to online activities that will support learning outcomes and educate the pupils in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation. Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work. They will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy. Pupils will use age-appropriate tools to research Internet content.

Use of Digital and Video Images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the Internet. However, staff, parents/carers and pupils need to be aware of the risks associated with publishing digital images on the Internet. Such images may provide avenues for cyber-bullying to take place. Digital

images may remain available on the Internet forever and may cause harm or embarrassment to individuals in the short or longer term. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm.

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing their own images on the Internet e.g. social networking sites.
- In accordance with guidance from the Information Commissioner's office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases, protection, parents/carers will be informed that such material is for their personal use only and should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other pupils in the digital/video images.
- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images.
- Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used in association with photographs on the school website.
- Written permission from parents/carers will be obtained before photographs of pupils are published on the school website/Facebook pages.

Use of Email and School Website

Email is an essential means of communication for both staff and pupils. Directed email use can bring significant educational benefits; interesting projects between schools can be created for example.

Email will be managed by ensuring that:

- Pupils may only use approved email accounts for school purposes
- Pupils must immediately tell a member of staff if they receive offensive email
- Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult

- Staff will only use official, school provided email accounts to communicate with pupils and parents, as approved by the Senior Management Team
- Access in school to external personal email accounts may be blocked
- Emails sent to external organisations should be written in a professional manner
- Staff should not use personal email accounts during school hours or for professional purposes

Abbey Primary School's Website celebrates pupils' work, promotes the school and publishes resources for projects. The contact details on the website will be the school address, email and telephone number. Staff or pupils' personal information will not be published. The principal will take overall editorial responsibility for online content published by the school and will ensure that content published is accurate and appropriate. The school website will comply with the school's guidelines for publications including respect for intellectual property rights, privacy policies and copyright. The security of staff and pupils is paramount.

Use of Internet Access

Abbey Primary School requests parental permission before a child can be granted Internet access. We are aware that pupils should not be prevented from accessing the Internet unless the parents have specifically denied permission.

In order to ensure safe Internet access,

- all staff will read and sign the school Acceptable Use Policy (AUP) before using any school ICT resources
- parents will be asked to read the School Acceptable Use Policy for pupil access, discuss it with their child, sign and return to school
- any visitors to the school site who require access to the school's network or internet access will be asked to read and sign an Acceptable Use Policy
- parents will be informed that pupils will be provided with supervised Internet access appropriate to their age and ability
- consideration will be given regarding vulnerable members of the school community (such as children with special educational needs). The school will make decisions based on the specific needs and understanding of the pupil(s)
- at Foundation Stage and Key Stage 1, pupils' access to the Internet will be by adult demonstration with occasional directly supervised access to specific and approved online materials
- at Key Stage 2 pupils will be supervised. Pupils will use age-appropriate search engines and online tools with online activities being teacher- directed where necessary

The school will take all reasonable precautions to ensure that users access only appropriate material. ICT use will be audited to establish if the e-Safety Policy is adequate and that the implementation of the e-Safety Policy is appropriate. Methods to identify, assess and minimise risks will be reviewed regularly.

Use of Mobile Phones and other personal devices

Mobile phones and other personal devices such as Games Consoles, Tablets, PDA, MP3 Players etc. are considered to be an everyday item in today's society and even children in early years' settings may own and use personal devices to get online regularly. Mobile phones and other internet enabled personal devices can be used to communicate in a variety of ways with texting, camera phones and internet accesses all common features.

However, mobile phones can present a number of problems when not used appropriately:

- they are valuable items which may be stolen or damaged
- their use can render pupils or staff subject to cyberbullying
- internet access on phones and personal devices can allow pupils to bypass school security settings and filtering
- mobile phones with integrated cameras could lead to child protection, bullying and data protection issues with regard to inappropriate capture, use or distribution of images of pupils or staff
- the use of mobile phones and other personal devices by students and staff in school will be decided by the school and covered in the school Acceptable Use Policy
- the sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the school community and any breaches will be dealt with as part of the school discipline/behaviour policy
- mobile phones and personal devices should be silent during curriculum time
- electronic devices of all kinds that are brought into school or on residential trips are the responsibility of the user. The school accepts no responsibility for the loss, theft or damage of such items, nor will the school accept responsibility for any adverse health effects caused by any such devices either potential or actual
- if a member of staff breaches the school policy then disciplinary action may be taken

Monitoring and Filtering

Occasionally mistakes may happen and inappropriate content may be accessed. It is therefore important that children are always supervised when using Internet access and that Acceptable Use Policies are in place. In addition, Internet Safety rules will be displayed and both children and adults will be educated about the risks online. There will also be an Incident Log to report breaches of filtering or inappropriate

content being accessed. Teachers will always evaluate any websites/search engines before using them with their pupils; this includes websites shown in class as well as search results just before the lesson.

The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named within the “Roles and Responsibilities” section of this policy will be effective in carrying out their e-Safety responsibilities.

Procedures for monitoring and filtering will ensure that:

- school technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- the school’s access strategy will be designed by educators to suit the age and curriculum requirements of the pupils, with advice from network managers
- servers, wireless systems and cabling must be securely located and access restricted
- the school’s broadband access will include filtering appropriate to the age and maturity of pupils
- appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts, which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software
- all users will have clearly defined access rights to school systems and devices
- all users at Key stage 2 will be provided with a username and secure password. Users are responsible for the security of their username and password and will be required to change their password as required
- the administrator passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the Principal
- internet access is filtered appropriately for all users and there is a clear process in place to deal with requests for filtering changes
- if in the event of any material that may be deemed inappropriate appearing on any ICT device, the member of staff will immediately email the Principal (marked FILTERING INCIDENT REPORT in the email title). This will be passed to the e-Safety Co-ordinator
- temporary users (e.g trainee teachers, supply teachers, visitors etc.) will be subject to the policies when working on the school systems
- all school supplied ICT devices must be used appropriately in accordance with the school’s Acceptable Use Policy
- the Senior Management Team will ensure that regular checks are made to ensure that the filtering methods selected are effective
- any material that the school believes is illegal will be reported to appropriate agencies such as CEOP

- if staff or pupils discover unsuitable sites, the URL will be reported to the school e-Safety Co-ordinator who will then record the incident and escalate the concern as appropriate
- the school will have a clear procedure for reporting breaches of filtering. All staff and pupils will be aware of this procedure

Procedures should Incidents Occur

Internet technologies and electronic communications provide children and young people with exciting opportunities to broaden their learning experiences and develop creativity in and out of school. However, it is also important to consider the risks associated with the way these technologies can be used. At Abbey Primary School, we recognise and seek to develop the skills that pupils need when communicating and using technologies enabling them to keep safe and secure and act with respect for others. Teachers are the first line of defence; their observation of behaviour is essential in recognising concerns about pupils and in developing trust so that issues are reported.

Staff should also help develop a safe culture by observing each other's behaviour online and discussing together any potential concerns.

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible, or very rarely, through deliberate misuse.

In order to safeguard staff and pupils:

- 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 Co-ordinator will record all reported incidents and actions taken in the school e-Safety incident log and other in any related areas e.g. Anti-Bullying or Child Protection log
- the e-Safety Co-ordinator 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
- where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact the relevant authority

Parents, teachers and pupils should know how to use the school's complaints procedure. The facts of the incident or concern will need to be established and evidence should be gathered where possible and appropriate. E-Safety incidents may

have an impact on pupils, staff and the wider school community both on and off site and can have civil, legal and disciplinary consequences.

A minor transgression of the school rules may be dealt with by a member of staff. Other situations could potentially be serious and a range of sanctions may then be required, which should be linked to the school's disciplinary policy. Potential child protection or illegal issues must be referred to the school Designated Child Protection Officer or e-Safety Co-ordinator.

Complaints about Internet misuse will be dealt with under the school's complaints procedure.

Any complaint about staff misuse will be referred to the Principal.

All e-Safety complaints and incidents will be recorded by the school, including any actions taken.

- Pupils and parents will be informed of the complaints procedure.
- Parents will need to work in partnership with the school to resolve issues.
- All members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns.
- Any issues (including sanctions) will be dealt with according to the school's disciplinary, behaviour and child protection procedures.
- All members of the school 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 school community.

The following guidance is intended for use when members of staff need to manage incidents that involve inappropriate use of ICT devices. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities. In the event that a member of staff is unsure if an incident should be reported or not, the rule is, "When in doubt, always report the matter to the Principal."

In the event of suspicion, all steps in this procedure will be followed:

- More than one senior member of staff will be involved in the process. (This is vital to protect individuals, if accusations are subsequently reported).
- The procedure will be conducted using a designated computer that will not be used by pupils and if necessary, may be taken off site by the police, should the need arise. The same computer will be used for the duration of the procedure.

- The relevant staff should have appropriate Internet access to conduct the procedure and sites and content visited will be closely monitored and recorded (to provide further protection).
- The URL of any site containing the alleged misuse will be recorded as well as the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form. (Except in the case of images of child sexual abuse).
- Following the investigation, the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include internal response/disciplinary procedures, involvement by a local authority or police involvement/action.
- If contact being reviewed includes images of Child Abuse, then the monitoring will be halted and referred to the police immediately. Other instances to report to the police would include,

-incidents of “grooming” behaviour,

-the sending of obscene materials to a child

-adult material which potentially breaches the Obscene Publications Act

-criminally racist material

-other criminal conduct, activity or materials

- The computer in question will be isolated. Any change to its state may hinder any police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police. It will demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

Cyberbullying

Cyberbullying can be defined as, “The use of Information Technology, particularly mobile phones and the Internet to deliberately hurt or upset someone.” Many young people and adults find that using the Internet and mobile phones is a positive and creative part of their everyday life. Unfortunately, technologies can also be used negatively. When children are the target of bullying via mobile phones, gaming or the Internet, they can often feel very alone, particularly if the adults around them do not

understand cyberbullying and its effects. A once previously safe and enjoyable environment or activity can become threatening, harmful and a source of anxiety. It is essential that young people, school staff and parents / carers understand how cyberbullying is different from other forms of bullying, how it can affect people and how to respond and combat misuse. Promoting a culture of confident users will support innovation and safety. The guidelines below will be followed:

- Where bullying outside school (such as online or via text) is reported to the school, it will be investigated and acted on. Cyberbullying, as with any form of bullying, will not be tolerated at Abbey Primary School.
- All incidents of cyberbullying reported to the school will be recorded.
- There will be clear procedures in place to investigate incidents or allegations of cyberbullying.
- Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.
- The school will take steps to identify the bully, where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses and contacting the service provider and the police, if necessary.
- Pupils, staff and parents/carers will be required to work with the school to support the approach to cyberbullying and the school's e-Safety ethos.
- Sanctions for those involved in cyberbullying may include:
 - The bully will be asked to remove any material deemed to be inappropriate or offensive.
 - A service provider may be contacted to remove content if the bully refuses or is unable to delete content.
 - Internet access may be suspended at school for the user for a period of time.Other sanctions for pupils and staff may also be used in accordance to the school's Anti-Bullying, Behaviour Policy or Acceptable Use Policy.
- Parents/Carers of pupils will be informed.
- The police will be contacted if a criminal offence is suspected.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998, which states that personal data must be:

- fairly and lawfully processed
- processed for limited purposes
- adequate, relevant and not excessive
- accurate
- kept no longer than is necessary
- processed in accordance with the data subject's rights
- secure
- only transferred to others with adequate protection

The school must ensure that:

- it will hold the minimum personal data necessary to enable it to perform its function and it will not hold it longer than necessary for the purposes it was collected for
- every effort will be made to ensure that data is accurate, up to date and that inaccuracies are corrected without unnecessary delay
- it is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
- it has clear and understood arrangements for the security, storage and transfer of personal data
- data subjects have rights of access and there are clear procedures for this to be obtained
- there are clear and understood policies and routines for the deletion and disposal of data

When personal data regarding children is stored on any portable computer system, e.g. lap -top or i-Pad,

- the device must be password protected
- approved virus and malware checking software must be installed on the device
- the data must be securely deleted from the device once it has been transferred or its use is complete

Personal data relating to staff must not be stored on the school system or on school devices, which are intended for professional use only.

Communication of this policy to Pupils, Staff and Parents**Pupils**

- All pupils will be informed that network and Internet use will be monitored.
- All teachers will raise awareness of e-Safety across the school and stress and importance of safe and responsible Internet use amongst pupils.
- Pupil instruction regarding responsible and safe use will precede Internet access.
- e-Safety rules or copies of the Pupil Acceptable Use policy will be posted in all areas with Internet access.
- Safe and responsible use of the Internet and technology will be reinforced across the curriculum and subject areas.
- Particular attention to e-Safety education will be given where pupils are considered to be vulnerable.

Staff

It is important that all staff feel confident to use new technologies in teaching and the school e-Safety Policy will only be effective if all staff subscribe to its values and methods. Staff should be given opportunities to discuss the issues and develop appropriate teaching strategies.

Particular consideration must be given when members of staff are provided with devices by the school, which may be accessed outside of the school network. Schools must be clear about the safe and appropriate uses of their school provided equipment and have rules in place about use of the equipment by third parties. Staff must be made aware of their responsibility to maintain confidentiality of school information.

- The e-Safety Policy will be formally provided to and discussed with all members of staff.
- To protect all staff and pupils, the school 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 are essential.
- Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided to all members of staff.
- Staff who manage filtering systems or monitor ICT use will be supervised by the Senior Management Team and have clear procedures for reporting issues.
- The school will highlight useful online tools which staff will use with the children in the classroom. These tools will vary according to the age and ability of the pupils.
- All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.
- Staff of Abbey Primary will only use school provided devices for professional work. Third party users (e.g. family members or friends) are not permitted to use the device to ensure confidentiality of information and child protection.

Parents

- Parents' attention will be drawn to the school e-Safety Policy in newsletters, the school prospectus and on the school website.
- A partnership approach to e-Safety at home and at school with parents will be encouraged. This may include offering parent evenings with demonstrations and suggestions for safe home Internet use, or highlighting e-Safety at other attended events e.g. parent evenings and sports days.
- Advice on useful resources and websites will be given to parents.
- Information and guidance for parents on e-Safety will be made available to parents in a variety of formats.

- Parents will be requested to sign an Acceptable Use Agreement for pupils and discuss its implications with their children.

Monitoring and Evaluation of the e-Safety Policy

This e-Safety Policy has been developed by a working group consisting of;

- Principal – Designated Child Protection Officer
- Vice-Principal – Deputy Child Protection Officer and e-Safety Officer
- Senior Management Team
- ICT Co-ordinators and panel
- Staff

Consultation with the whole school community has taken place through a range of formal and informal meetings.

This e-Safety Policy was approved by the Board of Governors on _____.

The implementation of the policy will be monitored by the Principal, Senior Management Team, e-Safety Co-ordinator and ICT Co-ordinators.

Monitoring of the policy will take place annually in May, or more regularly in light of any significant new developments in the use of the technologies, new threats to e-Safety or incidents that have taken place.

The Board of Governors will receive an annual update of the policy every May.

The next anticipated review date will be June 2017.

Should serious e-safety incidents take place, SEELB should be informed.

The school will monitor the impact of the policy using logs of reported incidents and department guidelines/circulars.

Abbey Primary School (September 2016)

Review Date: June 2017