Benson School
eSafety Policy

SAFEGUARDING OUR PUPILS
AND STAFF IN A DIGITAL WORLD

SEPTEMBER 2012

Table of Contents:

Introduction

This eSafety policy recognises our commitment to e-safety and acknowledges its part in the school's overall Safeguarding policies and procedures. It shows our commitment to meeting the requirements to keep pupils safe in the 'Every Child Matters' agenda.

We believe our 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. Our expectations for responsible and appropriate conduct are formalised in our **Benson School Internet Codes of Conduct** which we expect all staff and pupils to abide by.

As part of our commitment to eSafety we also recognise our obligation to implement a range of security measures to protect the school network and facilities from attack, compromise and inappropriate use and to protect school data and other information assets. We have adopted the good practice requirements for all staff which are included in the **Benson School Information, Security & Guidance section.**

For the purposes of clarity and consistency throughout this document the person in **Benson School** who is taking a lead on eSafety is called the **eSafety coordinator.**

The person at Benson School taking on the role of eSafety coordinator is the:

BENSON SCHOOL ICT COORDINATOR

This policy was generated by the:

BENSON SCHOOL SITE MANAGER

This Policy was originally generated on the:

06th October 2010

This Policy has been reviewed on the:

26th September 2012

This Policy has been approved by the:

BENSON SCHOOL GOVERNING BODY

The following local and national guidance are acknowledged and included as part of our eSafety policy:

1.

Benson School Information, Security & Guidance

Benson School Safeguarding, Procedures and Guidance

Benson School Safeguarding Procedures will be followed where an eSafety issue occurs which gives rise to any concerns related to Child Protection. In particular we acknowledge the specific guidance in:

Section 5.1.6 Child Abuse and Information Communication Technology

This section covers awareness of, and response to, issues related to child abuse and the Internet. In particular we note and will follow the advice given in the following section:

Section 7. Actions to be taken where an employee has concerns about a colleague
This provides guidance on the action to be taken if an employee has either information or reason to suspect that a colleague is accessing indecent images of children.

Guidance for Safer Working Practices for Adults who work with Children and Young People

This guidance provides clear advice on appropriate and safe behaviors for all adults working with children in paid or unpaid capacities, in all settings and in all contexts. We acknowledge the guidance given in the following sections and accept this as part of our policy. (See extract in Appendix)

- **Section 12 Communication with Children and Young People**
- **Section 27 Photography and Videos**
- **Section 28 Access to inappropriate images and Internet Usage**

2.

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 school community are able to benefit from the opportunities that technology provides for learning and teaching. The following responsibilities demonstrate how each member of the school community can contribute.

The Management Team accepts the following responsibilities:

- To identify a person (the eSafety coordinator) to take responsibility for eSafety and support them in their work.
- Ensure adequate technical support is in place to maintain a secure ICT system
- Ensure policies and procedures are in place to ensure the integrity of the school's information and data assets
- Ensure to liaise with the School Governing Body
- Develop and promote an eSafety culture within the Benson School Community
- Ensure that all staff and pupils agree to abide by the **Benson School Internet Codes of Conduct** and that new staff have eSafety included as part of their school induction procedures
- Make appropriate resources, training and support available to all members of the school community to ensure they are able to carry out their roles effectively with regard to eSafety
- 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
- To take ultimate responsibility for the eSafety of the school community

The responsibilities of the eSafety Coordinator are:

- To promote an awareness and commitment to eSafety throughout the school
- To be the first point of contact in school on all eSafety matters
- To lead the school eSafety meetings
- To create and maintain eSafety policies and procedures
- To develop an understanding of current eSafety issues, guidance and appropriate legislation

- To ensure delivery of an appropriate level of training in eSafety issues
- To ensure that eSafety education is embedded across the curriculum
- To ensure that eSafety is promoted to parents/guardians
- To ensure that any person who is not a member of school staff, who makes use of the school ICT equipment in any context, is made aware of the **Benson School Internet Codes of Conduct.**
- To liaise with the Local Authority, the Local Safeguarding Children's Board and other relevant agencies as appropriate
- To monitor and report on eSafety issues to the Senior Management Team and Board of Governors as appropriate
- To ensure that staff and pupils know the procedure to follow should they encounter any material or communication that makes them feel uncomfortable or that contravenes this ePolicy
- To ensure an eSafety incident log is kept and up to date
- To ensure that **Benson School Internet Codes of Conduct** for **eSafety** are displayed in appropriate areas around the site

The responsibilities of all staff are:

- To read, understand and help promote the school's **Benson School Internet Codes of Conduct**
- To take responsibility for ensuring the safety of sensitive school data and information
- To develop and maintain an awareness of current eSafety issues and legislation and guidance relevant to their work
- To maintain a professional level of conduct in their personal use of technology at all times
- To embed eSafety messages in learning activities where appropriate
- To supervise pupils carefully when engaged in learning activities involving technology
- To ensure that pupils are told what to do should they encounter any material or receive a communication which makes them feel uncomfortable
- To report all eSafety incidents which occur in the appropriate log and/or to their line manager
- To respect the feelings, rights, values, beliefs and intellectual property of others in their use of technology in school and at home

The additional responsibilities of technical staff are:

- To support the school in providing a safe technical infrastructure to support learning and teaching
- To ensure appropriate technical steps are in place to safeguard the security of the Benson School ICT system, sensitive data and information. Review these regularly to ensure they are up to date
- To, at the request of the Leadership team conduct occasional checks on files, folders, email and other digital content to ensure that the **Benson School Internet Codes of Conduct** are being adhered too
- To report any eSafety related issues that come to light to the attention of the eSafety coordinator and/or the Safeguarding Officer if necessary
- To ensure that procedures are in place for new starters and leavers to be correctly added to and removed from all relevant electronic systems
- To ensure that suitable access arrangements are in place for any external users of the schools ICT equipment
- To liaise with the Local Authority and others on e-safety issues

The responsibilities of all pupils are:

- To read, sign as understood and abide by the **Benson School Internet Codes of Conduct** prior to internet access being granted
- To take responsibility for their own use of technology at all times
- To ensure they respect the feelings, rights, values, beliefs and intellectual property of others in their use of technology in school and outside of school
- To 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
- To report all eSafety incidents to appropriate members of staff
- To discuss eSafety issues with family and friends in an open and honest way

The responsibilities of parents/guardians are:

- To help and support Benson School in promoting eSafety at all times
- To read, understand and to sign the **Benson School Internet Codes of Conduct**
- To discuss the **Benson School Internet Codes of Contact** with their child/children and to show an interest in how they are using technology and to encourage them to behave safely and responsibly when using the internet
- To consult directly with Benson School if they have any concerns about their child's use of technology

The responsibilities of the Schools Governing Body are:

- To read, understand, contribute to and help promote Benson School's eSafety policies and guidance as part of the schools overarching safeguarding procedures
- To support the work of Benson 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 ensure appropriate funding and resources are available for Benson School to implement their eSafety strategy

3.

Benson School Internet Codes of Conduct

Benson School has **Internet Codes of Conduct** that all pupils and staff are required to read and sign prior to being given access to the schools internet system.

The pupil's parent/guardian must also sign to say that they agree with the **Benson School Internet Codes of Conduct** and that they are happy for their child/ children to use the school internet system.

Anyone failing to sign and return their completed form will not be given access to the school internet system.

4.

Learning and Teaching

Benson School believes that the key to developing safe and responsible behaviours online for everyone within our school community lies in effective education. We know that the Internet and other technologies are embedded in our pupils' lives, not just in school but outside as well, and we believe we have a duty to help prepare our pupils to benefit safely from the opportunities that these present.

We will deliver a planned and progressive scheme of work to teach eSafety knowledge and understanding and to ensure that pupils have a growing understanding of how to manage the risks involved in online activity.

We believe that learning about eSafety should be embedded across the curriculum and also taught in specific lessons such as ICT.

We will discuss, remind or raise relevant eSafety messages with pupils routinely wherever suitable opportunities arise.

We will remind pupils about their responsibilities to which they have agreed through the **Benson School Internet Codes of Conduct**.

5.

How parents/guardians will be involved

We believe it is important to help all our parents/guardians develop sufficient knowledge, skills and understanding to be able to help keep themselves and their children safe.

To achieve this we will offer opportunities for finding out more information through meetings, the school newsletter and website.

6.

Managing and Safeguarding ICT Systems

The school will ensure that access to the school ICT system is as safe and secure as reasonably possible.

Servers and other key hardware or infrastructure are located securely with only appropriate staff permitted access. Servers, workstations and other hardware and software are kept updated as appropriate. A firewall is maintained and virus and malware protection is installed on all appropriate hardware and is kept active and up-to-date. Staff have virus protection installed on all laptops used for school activity.

Any administrator or master passwords for school ICT systems are kept secure.

Any future wireless network is protected by a secure log on which prevents unauthorized access. New users can only be given access by nominated individuals.

We do not allow anyone except technical staff to download and install software onto the network. Staff are allowed administrator rights to download software on school provided laptops.

Filtering Internet access

Web filtering of internet content is provided by the Local Educational Authority (LEA). This ensures that all reasonable precautions are taken to prevent access to inappropriate material. However it is not possible to guarantee that access to unsuitable material will never occur. Teachers are encouraged to check out websites they wish to use. All users are informed about the action they should take if inappropriate material is accessed or discovered on a computer.

Access

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 security systems in place for managing network accounts and passwords, including safeguarding administrator passwords.

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 authorised users only, with proper procedures being followed for authorising and protecting login and password information.

Remote access to school systems is covered by specific agreements and must never be allowed to be used by an unauthorised third party user.

Detailed guidance on the protection of sensitive school data and information assets is included in the **Benson School Information, Security & Guidance** which forms part of this policy.

7.

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 LEA, the examination boards and others

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

All users of the school ICT or electronic equipment will abide by the relevant **Benson School Internet Codes of Conduct** at all times, whether working in a supervised activity or working independently,

Pupils and staff are made fully aware of the actions that will be taken if inappropriate material is discovered and the consequences that these findings may involve.

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. There are systems in place for storing relevant electronic communications which take place between school and parents.

Use of the school e-mail system is monitored and checked.

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.

Responsible use of personal web mail accounts by staff is permitted.

Publishing content online

School website:

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

The contact details on the web site must only be the school address, e-mail and telephone number.

Identities of pupils are protected at all times. Photographs of identifiable individual pupils are not published on the web site and school obtains permission from parents for the use of pupils' photographs. Group photographs do not have a name list attached.

Creating online content as part of the curriculum:

As part of the curriculum we encourage pupils to create online content. Pupils are taught safe and responsible behaviour in their creation and publishing of online content. They are taught to publish for a wide range of audiences which might include governors, parents/guardians or younger children.

The publishing of online content by pupils will take place within the school learning platform or other media selected by the school. Pupils will only be allowed to post or create content on sites where members of the public have access, when this is part of a school related activity. Appropriate procedures to protect the identity of pupils will be followed.

We take all steps to ensure that any material published online is the author's own work, gives credit to any other work included and does not break copyright rules.

Online material published outside the school:

Staff and pupils are encouraged to adopt similar safe and responsible behaviours in their personal 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 recognise 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; images and video are of appropriate activities and are only taken of pupils wearing appropriate dress. Full names of participants are not used either within the resource itself, within the file-name or in accompanying text online.

School performances, plays, shows, etc may be recorded. However pupils will be consulted before the recording etc takes place. No pupil's role or part in any performance or event would be jeopardised because they do not want to be photographed or recorded.

Using other technologies

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

We will review the eSafety policy when necessary or inline with Oxfordshire County Council Directives. Or due to the introduction of any new technology that may not be covered by this policy.

Staff or pupils using a new technology not specifically mentioned in this policy will be expected to behave with similar standards of behavior to those outlined within this document.

8.

Protecting school data and information

Benson School recognises its obligation to safeguard staff and pupil's personal data including that which is stored and transmitted electronically. We regularly review our practices and procedures to ensure that they meet this basic obligation.

The school is a registered Data Controller under the Data Protection Act 1998 and we comply at all times with the requirements of that registration.

Pupils are taught about the need to protect their own personal data as part of the **Benson School Internet Codes of Conduct** and have to sign an agreement form stating that they will abide by the codes prior to being given access to the internet.

Staff are made fully aware of the contents of the **Benson School Information, Security & Guidance** section which is included as part of this policy.

Suitable procedures, and where necessary training, are in place to ensure the security of such data including the following:

- Staff must be provided with personal USB memory sticks for carrying sensitive data
- All computers or laptops holding sensitive information are password protected and staff are aware that all computers must be locked when they are left unattended
- Staff are provided with appropriate levels of access to the schools management information systems holding pupil data. Passwords are not shared and administrator passwords are kept by each member of staff individually
- Staff are aware of their obligation to keep sensitive data secure when working on computers outside school
- When we dispose of old computers and other equipment we take due regard for destroying information which may be held on them
- Remote access to computers is only allowed during updating of the server and this is done by authorised ICT personnel
- We have full back up and recovery procedures in place for school data
- Sensitive staff or pupil data is only accessible to people who have a right to see the information, for example Governors or the local Educational Authority Representatives (security cleared), they are reminded on receiving the information of their duty to keep it safe and secure and that it is not to be seen or discussed with any third party.

9.

Dealing with eSafety incidents

All eSafety incidents should be recorded in the School eSafety Log which should be regularly reviewed.

Any incidents where pupils do not follow the **Benson School Internet Codes of Conduct** will be dealt with following the school's normal behaviour or disciplinary procedures.

In situations where a member of staff is made aware of a serious eSafety incident, concerning pupils or staff, they will inform the eSafety coordinator or if necessary the Benson School Safeguarding Officer, who will then respond in the most appropriate manner. [See **First Response Guidance to eSafety Incidents]**

Instances of **cyberbullying** will be taken very seriously by the school and dealt with using the schools anti-bullying procedures. Benson School recognises that staff as well as pupils may be victims and will take appropriate action in either situation.

(Cyberbullying will not be tolerated)

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

Dealing with a Child Protection issue arising from the use of technology:

If an incident occurs which raises concerns about Child Protection or the discovery of indecent images on the computer, then the procedures outlined in the Benson School Safeguarding Procedures and Guidance will be followed.

Section 5.1.6 Child Abuse and Information Communication Technology

Dealing with complaints and breaches of conduct by pupils:

- Any complaints or breaches of **Benson School Internet Codes of Conduct** will be dealt with promptly under the school discipline system
- Responsibility for handling serious incidents will be given to a senior member of staff
- A initial fact finding investigation must be carried out

- Parents and the pupil will work in partnership with staff to resolve any issues arising
- 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 behavior 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, any form of cyberbulling will not be tolerated
- 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 are likely to result in disciplinary action:

- any online activity by a member of the school community which is likely to adversely impact on the reputation of the school
- accessing inappropriate or illegal content accidentally and failing to report this
- inappropriate use of personal technologies (e.g. mobile phones) at school or in lessons
- sharing files which are not legitimately obtained e.g. music files from a file sharing site
- using school or personal equipment to send a message, or create content, that is offensive or bullying in nature or could bring the school into disrepute
- attempting to circumvent LEA, school filtering, monitoring or other security systems
- circulation of commercial, advertising or 'chain' emails or messages
- revealing the personal information (including digital images, videos and text) of others by electronic means (e.g. sending of messages, creating online content) without permission
- using online content in such a way as to infringe copyright or which fails to acknowledge ownership (including plagiarising of online content)
- transferring sensitive data insecurely or infringing the conditions of the Data protection Act, revised 1988
- 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 persona 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

10.

References to related documents:

- **Benson School Internet Codes of Conduct (Pupils, Staff, Visitors, Supply Staff and any other service users)**
- **Letter to parents explaining the Benson School Internet Codes of Conduct and asking for signature of agreement/permission**
- **Benson School Information Security Guidance for Staff**
- **First Response Guidance to eSafety Incidents (Safeguarding)**
- **Practical Guidance for Protecting School Information**
- **Guidance for using children's work in publications and on web sites**

11.

Further resources

There is a comprehensive eSafety section available on the Oxford County Council website

12.

Appendix

Extract from:

Guidance for the Safer Working Practice for Adults who work with Children and Young People.

Section 12 Communication with Children and Young People *(including the Use of Technology)*

Communication between children and adults, by whatever method, should take place within clear and explicit professional boundaries. This includes the wider use of technology such as mobile phones text messaging, e-mails, digital cameras, videos, web-cams, websites and blogs. Adults should not share any personal information with a child or young person. They should not request, or respond to, any personal information from the child/young person, other than that which might

be appropriate as part of their professional role. Adults should ensure that all communications are transparent and open to scrutiny.

Adults should also be circumspect in their communications with children so as to avoid any possible misinterpretation of their motives or any behaviour which could be construed as grooming. They should not give their personal contact details to children and young people including e-mail, home or mobile telephone numbers, unless the need to do so is agreed with senior management and parents/guardians. E-mail or text communications between an adult and a child young person outside agreed protocols may lead to disciplinary and/or criminal investigations. This also includes communications through internet based web sites.

(Communication systems should only be used in accordance with the schools policies)

This means that Benson School should:

- *have a communication policy which specifies acceptable and permissible modes of communication*

Underlining to staff that they should:

- *never give their personal contact details to a children or young people, including their mobile telephone number and details of any blogs or personal websites*
- *only use communication equipment e.g. mobile phones, provided by Benson School for work purposes and never to communicate with pupils or young persons*
- *only make contact with children for professional reasons and in accordance with any Benson School Policy as part of your work commitment*
- *be aware of the inappropriate forms of contact with a pupil at all times*
- *not use internet or web-based communication channels to send personal messages to a child or young person*

Section 27 Photography and Videos

Working with children and young people may involve the taking or recording of images. Any such work should take place with due regard to the law and the need to safeguard the privacy, dignity, safety and well being of children and young people. Informed written consent from parents/guardians and agreement, where possible, from the child or young person, should always be sought before an image is taken for any purpose.

Careful consideration should be given as to how activities involving the taking of images are organised and undertaken. Care should be taken to ensure that all parties understand the implications of the image being taken especially if it is to be used for any publicity purposes or published in the media, or on the Internet. There also needs to be an agreement as to whether the images will be destroyed or retained for further use, where these will be stored and who will have access to them.

Adults need to remain sensitive to any children who appear uncomfortable, for whatever reason, and should recognise the potential for such activities to raise concerns or lead to misunderstandings.

It is not appropriate for adults to take photographs of children for their personal use.

This means that staff should:

- *be clear about the purpose of the activity and about what will happen to the images when the activity is concluded*
- *be able to justify any images of children*
- *avoid making images in one to one situations or which show a single child with no surrounding context*
- *ensure the child/young person understands why the images are being taken and has agreed to the activity and that they are appropriately dressed.*
- *only use equipment provided or authorised by Benson School*
- *report any concerns about any inappropriate or intrusive photographs found*
- *always ensure they have parental permission to take and/or display photographs of a pupil/child*

This means that adults should not:

- *display or distribute images of children unless they have consent to do so from parents/guardians*
- *use images which may cause distress*
- *use mobile telephones (school or personal) to take images of children*
- *never take images 'in secret', or taking images in situations that may be construed as being secretive.*

Section 28 Access to Inappropriate Images and Internet Usage

There are no circumstances that will justify adults possessing indecent images of children. Adults who access and possess links to such websites will be viewed as a significant and potential threat to children. Accessing, making and storing indecent images of children on the internet is illegal. This will lead to criminal investigation and the individual being barred from working with children and young people, if proven.

Adults should not use equipment belonging to Benson School to access adult pornography; neither should personal equipment containing these images or links to them be brought into the workplace. This will raise serious concerns about the suitability of the adult to continue to work with children.

Adults should ensure that children and young people are not exposed to any inappropriate images or web links. Benson School and adults need to ensure that internet equipment used by children have the appropriate controls with regards to access. e.g. personal passwords should be kept confidential.

Where indecent images of children or other unsuitable material are found, the **Benson School Safeguarding Officer**,**Mrs Helen Crolla, Headteacher)** must be informed immediately. She will then inform the **Police and Local Authority Designated Officer (LADO)**. At **no** time should anyone attempt to investigate the matter or evaluate the material themselves, as this may lead to evidence being contaminated which in itself can lead to a criminal prosecution.

This means that Benson School should

- *have a clearly defined Internet Codes of Conduct Policy*
- *have clear e-safety policies in place about access to and use of the internet*
- *make guidance available to both staff, children and young people about appropriate usage.*

This means that staff should:

- *adhere to the **Benson School Internet Codes of Conduct***

- *follow the Benson School Guidance on the use of IT equipment*
- *ensure that children are not exposed to unsuitable material on the internet*
- *ensure that any films or material shown to children and young people are age appropriate*

IMPORTANT INFORMATION:

The Benson School Board of Governors and Management reserve the right to alter this ePolicy at any time and without prior notice, in line with any new Legislation, Government or Local Educational Authority Directives or due to the introduction of any new technology that may affect the way that we use the internet.

Signed: **Mrs Helen Crolla - Head Teacher**

Signed: **Mr A Wood - Chair of Governors**

ePolicy generated and reviewed by:

Mr I Burtenshaw
Benson School
Site Manager