E-SAFETY POLICY

Introduction

It is the duty of schools to ensure that children are protected from potential harm both within and beyond the school environment. Therefore, the involvement of children, young people and parent/carers is also vital to the successful use of online technologies. This Policy has been updated to take into account the 2018 "Working Together To Safeguard Children" and the 2018 "Keeping Children Safe in Education" guidance.

Aims

This policy aims to explain how parents/carers, children or young people can be a part of these safeguarding procedures. It also details how children are educated to be safe and responsible users capable of making good judgements about what they see, find and use. The term 'e-safety' is used to encompass the safe use of all technologies in order to protect children, young people and adults from potential and known risks.

- To emphasise the need to educate staff and children about the pros and cons of using new technologies both within and outside School.
- To provide safeguards and agreement for acceptable use to guide all users, whether staff or students, in their online experiences.
- To ensure adults are clear about procedures for misuse of any technologies both within and beyond the School.
- To develop links with parents/carers and the wider community, ensuring input into policies and procedures with continued awareness of the benefits and potential issues related to technologies.

Roles and Responsibilities of the School

Headmaster's Responsibilities

It is the overall responsibility of the Headmaster to ensure that there is an overview of e-Safety as part of the wider remit of safeguarding across the School with further responsibilities as follows:

- The Headmaster has designated an e-Safety Lead to implement agreed policies, procedures, staff training and curriculum requirements and to take responsibility for ensuring e-Safety is addressed in order to establish a safe ICT learning environment. All staff and students are aware that **Colonel Keith Boulter**[AMD1] is the DSL (Designated Safeguarding Lead).
- Time and resources should be provided for the e-Safety Lead and staff to be trained and update policies, where appropriate.
- The Headmaster is responsible for promoting e-Safety across the curriculum together with the e-safety lead, Mrs Angela Dobson. There is a section in the computing policy development plan about e-safety.

- The School must ensure that any misuse or incident has been dealt with appropriately, according to policy and procedures, and appropriate action is taken, even to suspending a member of staff, informing the police (via establishment's agreed protocols with the police) or involving parents/carers.

The e-Safety Leads

The E Safety Lead in Barnardiston Hall is Mrs Angela Dobson, who has the support of ITEXS, the School's network support company. Mrs Dobson has completed e-safety lead training organised by E-Safety Suffolk.

It is the role of the designated e-Safety Lead to:

- Challenge the School about having:
    - Firewalls.
    - Anti-virus and anti-spyware software.
    - Filters.
    - Using an accredited ISP (internet Service Provider).
    - Awareness of wireless technology issues.
    - A clear policy on using personal devices.
- Appreciate the importance of e-safety within School and to recognise that all educational establishments have a general duty of care to ensure the safety of their pupils and staff.
- Establish and maintain a safe ICT learning environment within the School.
- Ensure that the Policy is reviewed annually, with up-to-date information, and that training is available for all staff to teach e-Safety and for parents to feel informed and know where to go for advice.
- Ensure that filtering is set to the correct level for staff and children in the initial set-up of a network, stand-alone PCs, staff/children's laptops and the learning platform or ensure the technician is informed and carries out work as directed.
- Ensure that all adults are aware of the filtering levels and why they are there to protect children.
- Report issues and update the SMT at least termly and when need arises. Liaise with the PSHEE, Safeguarding and ICT leads so that policies and procedures are up-to-date to take account of any emerging issues and technologies.
- Update staff training (all staff) according to new and emerging technologies so that the correct e-safety information can be taught or adhered to.
- Ensure transparent monitoring of the Internet and online technologies.
- Keep a log of incidents for analysis to help inform future development and safeguarding where risks can be identified.
- Ensure there is appropriate and up-to-date anti-virus software and anti-spyware on the network, stand-a-lone PCs and teacher/child laptops and that this is reviewed and updated on a regular basis.
- Ensure that staff can check for viruses on laptops, stand-a-lone PCs and memory sticks or other transferable data files to minimise issues of virus transfer.

- Ensure that unsolicited e-mails to a member of staff from other sources are minimised. Refer to the Managing Allegations Procedure, SSCB, for dealing with any issues arising from indecent or pornographic/child abuse images sent/received.
- Ensure there is regular monitoring of internal e-mails, where:
    - Blanket e-mails are discouraged
    - Tone of e-mails is in keeping with all other methods of communication
- Report overuse of blanket e-mails or inappropriate tones to the Headmaster.

STAFF TRAINING

Staff receive Workforce Awareness Training, which is a 1.5-hour course to raise awareness and improve e-safety within the education setting. It has been developed by Suffolk County Council's Safeguarding Learning and Quality Assurance Service and is delivered by Mrs Angela Dobson who is the overall Designated e-safety lead in School. Colonel Keith Boulter (Headmaster) takes overall responsibility for e-safety in the School.

RAISING PARENT AWARENESS

Information evenings or online seminars focussing on e-safety are made available to parents annually.

CHILDREN'S MOBILE PHONES / CAMERA / LAPTOPS / TABLETS

Mobile phones must not be used in School, on trips or at any time for the sending of text, e-mails or images which are unsuitable, or might be intimidating, to any other party. The School's wireless network must not be used to access social media sites or for anything other than directed work during the School Day.

Boarders may access their phones after supper and at designated times during the weekend. These are collected in before bedtime and kept in a locked cabinet. Any misuse of mobile phones will result in sanctions being taken including confiscation. Boarders' phones are checked periodically by boarding staff for inappropriate apps and games.

Children are made aware of internet safely through work in PSHEE and IT lessons.

If a child is in receipt of unsuitable material, it should be reported to an adult, who will then inform the DSL who may report it to CEOP.

Staff or Adults

All staff must undertake e-safety workforce training – a one and a half-hour certified course developed and updated by SLQA, Suffolk Safeguarding with updated training as required. Face-to-Face training with the e-safety lead is held annually for all staff.

It is the responsibility of all adults within the School to safeguard children from harm:

- Be familiar with the Behaviour, Anti-Bullying and other relevant policies and report concerns.
- Check the filtering levels are appropriate for their children and are set at the correct level. Report any concerns.
- Alert the e-Safety Lead about any new or arising issues and risks that may need to be included within policies and procedures.
- Ensure that children are protected and supported in their use of technologies so that they know how to use them in a safe and responsible manner. Children should know what to do in the event of an incident.
- Be up-to-date with e-Safety knowledge that is appropriate for the age-group and reinforce through the curriculum.
- Sign an "Acceptable Use" Statement to show that they agree with, and accept, the agreement for staff using non-personal equipment within and beyond the School environment.
- Use electronic communications in an appropriate way that does not breach the General Data Protection Regulations. Remember confidentiality and know not to disclose information from the network, pass on security passwords or leave a station unattended when they, or another, user is logged in.
- Ensure that School follows the correct procedures for any data required to be taken from the School premises.
- Report accidental access to inappropriate materials to the e-Safety Lead in order that inappropriate sites are added to the restricted list or filter.
- Use anti-virus software and check for viruses on work laptops, memory sticks or CD ROMs when transferring information from the internet on a regular basis, especially when not connected to the School's network.
- Ensure that all personal storage devices (i.e. memory sticks) which are utilised by staff members to hold sensitive information, are encrypted or password-protected in the event of loss or theft.
- Ensure that all devices that may access School data such as OneDrive are password protected at all times so the data cannot be accessed in the event of theft or loss of a device.
- Report incidents of personally-directed "bullying" or other inappropriate behaviour via the Internet or other technologies to the SDL.
- Also – see separate EYFS Mobile phones and cameras policy.

Children

Children should be:

- Involved in the review of the **Acceptable Use Agreement** through the Prefects and the Pupils' Consultative Council.
- Responsible for following the Acceptable Use Agreement whilst in the School as agreed at the beginning of each Academic Year or whenever he or she attends the School for the first time.

- Taught to use the internet in a safe and responsible manner through computing lessons, PSHEE or other clubs and groups.
- Taught to tell an adult about any inappropriate materials or contact from someone they do not know straight away, without reprimand.
- Taught about what is acceptable and unacceptable use of technology including what constitutes peer abuse such as “sexting”, “banter” and other forms of online bullying.

Appropriate and Inappropriate Use by Staff or Adults

Staff members have access to the network so that they can obtain age-appropriate resources for their classes and create folders for saving and managing resources. All staff should receive a copy of the Acceptable Use Policy and a copy of the Acceptable Use Agreement, which they need to sign and return to the School to keep on file.

In the Event of Inappropriate Use by Staff

If a member of staff is believed to misuse the internet or learning platform in an abusive or illegal manner, a report must be made to the Headmaster / Safeguarding Designated Lead immediately and then the Managing Allegations Procedure and the Safeguarding Policy must be followed to deal with any misconduct and all appropriate authorities contacted. In the lesser event of misuse or accidental misuse, this should be referred to the DSL and noted. Advice will be sought from the Suffolk LSCB when guidance is required on how to handle a case of inappropriate use.

Appropriate and Inappropriate Use by Children

Acceptable Use Agreements detail how children are expected to use the internet and other technologies within School, including downloading or printing of any materials.

The agreements are there for children to understand what is expected of their behaviour and attitude when using the internet. This will enable them to take responsibility for their own actions. For example, knowing what is polite to write in an e-mail to another child, or understanding what action to take should there be the rare occurrence of sighting unsuitable material. This also includes the deliberate searching for inappropriate materials and the consequences of doing so.

The agreement is on display within the classrooms and computer suite.

School should encourage parents or carers to support the agreement with their child or young person.

This is shown by signing the Acceptable Use Agreements together, so that it is clear to the School that the Agreement is accepted by the child with the support of the parent.

It is also intended to provide support and information to parents when children may be using the Internet outside School. It is hoped that parents will inform School of any potential issues that they feel should be addressed.

File-sharing via e-mail, weblogs, the downloading of materials, for example, music files and photographs, need to be appropriate and 'fit for purpose' based on research for work and be copyright-free.

Those children who are considered not able to understand or apply the e-safety policy either because they are too young, or due to SpLD, will not sign the agreement, but will not use the internet without very close supervision where they are directed to specific sites under the guidance or a member of staff. This will include all children in the Pre-Prep and a small number of children in the Prep School.

Action In the Event of Inappropriate Use

Should a child or young person be found to misuse the online facilities whilst at School, the following will happen:

- Any child found to be misusing the internet by not following the Acceptable Use Agreement may have a letter sent home to parents explaining the reason for suspending the child or young person's use for a particular lesson or activity. Boarders may have their use of electronic devices withdrawn for a period of time.
- Further misuse may result in not being allowed to access the internet for a period of time and another letter will be sent home to parents.
- A letter will be sent to parents outlining the breach in Safeguarding Policy where a child or young person is deemed to have misused technology against another child or adult. The Headmaster will also take appropriate disciplinary action.
- Advice will be sought from the Suffolk LSCB when guidance is required on how to handle a case of inappropriate use.

In the event that a child or young person accidentally accesses inappropriate material, the child should report this to an adult immediately and take action to hide the screen or close the window without deleting it, so that an adult can take the appropriate action to filter the site.

Where a child or young person feels unable to disclose abuse, sexual requests or other misuses against them to an adult, they can use the Report Abuse button (www.thinkuknow.co.uk) to make a report and seek further advice. Children must be made aware that this button alerts the Police to potentially abusive sites.

Deliberately misusing online technologies will be taken very seriously indeed by the School and parents will always be contacted.

Children should be taught and encouraged to consider the implications of misusing the internet and posting inappropriate materials to websites - for example, this may have legal implications.

The Curriculum and Tools for Learning

Internet Use

Barnardiston Hall, with parents, should teach children how to use the Internet safely and responsibly. They should also be taught, through computing and/or PSHE lessons, how to research information, explore concepts and communicate effectively in order to further learning.

The following concepts, skills and competencies should have been taught by the time pupils leave Form VI:

- Internet literacy.
- Making good judgements about websites and e-mails received.
- Knowledge of risks such as viruses and opening mail from a stranger.
- Access to resources that outline how to be safe and responsible when using any on-line technologies.
- Knowledge of copyright and plagiarism issues.
- Knowledge of inappropriate file-sharing and downloading illegal content and its consequences.
- Uploading information – to know what is safe to upload and not to upload regarding personal information.
- Where to go for advice and how to report abuse.

These skills and competencies are taught within both the PSHEE and computing curricula so that children have the security to explore how on-line technologies can be used effectively, but in a safe and responsible manner. Amongst other resources, the School uses the Gooseberry Planet materials which help to track the progress pupils are making against objectives.

Children should know how to deal with any incidents with confidence, as Barnardiston adopts the 'never blame the child for accidentally accessing inappropriate materials' culture in the event that they have **accidentally** accessed something.

For personal safety, we must ensure information uploaded to web sites and e-mailed to other people does not include any personal information such as:

- Full name (first name is acceptable, without a photograph).
- Address.
- Telephone number.
- E-mail address.
- School.
- Clubs attended and where.
- Age or DOB.

- Names of parents.
- Routes to and from School.
- Identifying information, e.g. I am number 8 in the School Rugby Team.

Photographs of children in School or on Out and Abouts or external activities should only be uploaded by the School Office from the designated computer and should only contain something which would also be acceptable in 'real life'. Parents should monitor the content of photographs uploaded. Images of children should be taken only with the School camera and stored only on the office computer (Mrs Fuller's) where they are downloaded. Parents taking photographs on sports days, at plays and concerts should be made aware of the School policy on recorded images and they should never be shared in the public domain.

Pupils with Additional Learning Needs

Barnardiston will strive to provide access to a broad and balanced curriculum for all learners and recognise the importance of tailoring activities to suit the educational needs of each pupil. Where a student has specific learning requirements, or poor social understanding, careful consideration is given to the planning and delivery of e-safety awareness sessions and internet access.

Social Media

Staff or adults need to ensure they consider the risks and consequences of anything they or their children may post to any web or social networking sites, as inappropriate comments or images can reflect poorly on an individual and can affect future careers.

It is illegal in the UK to have a Facebook presence before the age of 13. The School filter excludes Facebook and other known social media sites. However, if children are provided with 3G or 4G devices, whilst the School will do its best, it cannot ensure that children are using the internet safely and appropriately.

Parents must ensure that their children's privacy settings are appropriate and that personal details or anything that will put a child (Under 18) at risk is not posted online. Once a video / photograph / comment is posted, it is nearly impossible to remove and it will be there for life.

Children should be advised by parents on social networking security and recommendations made for privacy settings to be activated to 'Friends only' for all applications to restrict unsolicited access. The importance of passwords and blocking unwanted communications is also highlighted.

Adults should be aware that social networking can be a vehicle for cyber-bullying. Pupils are encouraged to report any incidents of bullying to the School, allowing for the procedures, as set out in the Anti-Bullying Policy, to be followed.

School Website

The uploading of images to the School website should be subject to the same acceptable agreement as uploading to any personal online space. Permission is gained from parents for the School to use photographs of the children at the registration stage via a GDPR Compliance Form. The School will consider which information is relevant to share with the general public on a website

External Websites

In the event that a member of staff finds himself or herself or another adult on an external website, such as 'Rate My Teacher', as a victim, this must be reported to the Headmaster and the School will report incidents to Social Services or the Police.

E-mail Use

Barnardiston has e-mail addresses for children(internal only) staff as a part of its entitlement to being able to monitor usage. Individual e-mail accounts can be traced if there is an incident of misuse.

Staff and childrenshould use their School-issued email addresses for School business only. A breach of this may be considered a misuse. Children's accounts are setup so they can only e-mail internally. Copies of all emails are stored in accordance with Data Protection Regulations.

Parents are encouraged to be involved with the monitoring of emails sent, although the best approach with children is to communicate about who they may be talking to and assess risks together.

The Network Manager has monitoring software that is used to flag up any inappropriate terms used and the Headmaster is always informed.

Mobile Phones and Other Emerging Technologies

Barnardiston carefully considers how the use of mobile technologies can be used as a teaching and learning tool within the curriculum with the following areas of concern taken into consideration:

- *Inappropriate or bullying text messages.*
- *Images or video taken of adults or peers without permission being sought.*
- *'Happy slapping' – the videoing of violent or abusive acts towards a child, young person or adult.*
- *Sexting - the sending of suggestive or sexually explicit (not necessarily involving nudity) personal images via mobile phones.*
- *Wireless Internet access, which can bypass School filtering and allow access to inappropriate or potentially harmful material or communications.*

Barnardiston does not permit mobile phones to be brought into School by day pupils unless there is a specific need which has been agreed with the Headmaster; this includes Out and Abouts and sports fixtures. There is always a School mobile phone available.

Boarders may have a mobile phone and other mobile devices for use between the end of Prep and Bedtime, with the consent of the senior member of staff on duty. These are locked away during the academic day and at night-time. Misuse of mobile devices will result in appropriate action taken and in a period of confiscation.

Children should understand the use of a public domain and the consequences of misuse. Relevant curriculum links are made to highlight the legal implications and the involvement of law enforcement.

Other technologies which are used with children include:

- Photocopiers.
- Tablets
- Telephones.
- Cameras (still and video)
- Smart Watches

Personal Mobile Devices for Staff

Staff are allowed to bring in personal mobile phones or devices for their own use, but **must not use personal numbers, email addresses or Social Media accounts to contact children under any circumstances.**

- Staff must ensure that there is no inappropriate or illegal content stored on the device and should be aware that using features, such as video or sound recording, may be subject to the same procedures as taking images from digital or video cameras.
- Staff should be aware that games consoles such as the Sony Play Station, Microsoft Xbox, Nintendo Wii and DSi and other such systems have Internet access which may not include filtering. Before use within School, authorisation should be sought from the Headmaster.
- The School is not responsible for any theft, loss or damage of any personal mobile device.

School-Issued Mobile Devices

The management of the use of these devices is similar to those stated above but with the following addition:

- Where School has provided a mobile device to a member of staff, such as a laptop or mobile phone, only this equipment should be used to conduct School business outside the School environment.

Video and Photographs

The term 'image' refers to the taking of video footage or photographs via any camera or other technology, e.g. a mobile phone.

When in School there is access to:

- Stills Cameras (kept in the Main Office)
- Video Recorder (kept in the Science Lab)
- Mobile telephones (kept in the Main Office)
- Tablets (Early Years)

All photographic material must be downloaded ONLY onto the Main Office computer and designated computers in the Nursery and Pre-Prep; the storage cards are regularly erased.

The sharing of photographs via weblogs, forums or any other means online should only occur after permission has been given by a parent/carer or member of staff.

Photographs/images are used to identify children on the School MIS are not shared.

Any photographs or video clips uploaded should not have a file name of a child, especially where these may be uploaded to a School website. Photographs should only ever include the child's first name although safeguarding guidance states either a child's name or a photograph but not both.

Group photographs are preferable to individual children's photographs and should not be of any compromising positions or in inappropriate or unsuitable clothing. All photographs are stored centrally on the Main Office computer only.

Video-Conferencing and Webcams

Publicly accessible webcams are not used in School.

Taking images via a webcam should follow the same procedures as taking images with a digital or video camera.

Children need to tell an adult immediately of any inappropriate use by another child or adult (this is part of the Acceptable Use Agreement).

Where children, young people (or adults) may be using a webcam in a family area at home, they should have open communications with parents/carers about their use and adhere to the Acceptable Use Agreement.

Web cams are occasionally (rarely) used by boarders with parents working overseas for contact by Skype at the request of the parent and under the supervision of a member of staff in an office area. Boarders may use Facetime or other such Apps to contact friends and parents via the School wifi.

Social Networking Advice for Staff

Social networking outside of work hours, on non-School issued equipment, is the personal choice of all School staff. Owing to the public nature of such websites, it is advisable for staff to consider the possible implications of participation. The following advice should be considered if involved in social networking:

- Personal details are never shared with pupils such as private email address, telephone number or home address. It is recommended that staff ensure that all possible privacy settings are activated to prevent students from making contact on personal profiles. The simplest and most effective way to do this is to remove details from search results and turn off public visibility.
- Staff should not engage in personal online contact with students outside of Headmaster-authorised systems (e.g. School e-mail account for homework purposes).
- Staff should ensure that full privacy settings are in place to prevent students from accessing photo albums or personal information.
- Staff are advised against accepting invitations from colleagues until they have checked with them in person that the invitation is genuine (avoiding fake profiles set up by students).
- Staff must not divulge personal information, such as private email addresses, telephone numbers or communicate with pupils on social networking sites until a pupil (or former pupil) has reached 18 years of age.
- Staff should not conduct any contact with Parents about School business or Pupils via Social Media. School e-mail addresses or School phones should be used for this.
- Staff should not post any pictures of Pupils on Social Media, nor comment or post in any way that could bring the good name of the School into disrepute.
- There is well-documented evidence to suggest that social networking can be a highly effective tool for communicating with students on a **professional** level. Barnardiston Hall has set up a Facebook account to manage and monitor public and pupil communications through **Mrs L P Gundersen**, the designated member of staff.

Safeguarding Measures – Filtering and Monitoring

Staff and children are required to use the personalised learning space, and all tools within it, in an acceptable way in accordance with the Acceptable Use Agreement for Staff and Pupils which everybody from Form I upwards has signed.

Barnardiston Hall uses a two-tier technical approach to internet safety in addition to the lessons taught to children in PSHE and Computing lessons. Firstly, OpenDNS provides Web content filtering as well as security and this is set up across all computers on the network, with two different levels of filtering for office computers and machines that could be

accessed by children. In addition, all computer use is monitored by Impero which is compliant with the UK Safer Internet Centre's 'appropriate monitoring' provider checklist. This includes active monitoring and logging incident captures to provide contextual insight, and helps The School to identify potential risk, respond before an incident escalates, and to educate students about responsible internet behaviour.

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

A firewall ensures information about children and the School cannot be accessed by unauthorised users.

Children should use a search engine that is age-appropriate. Google Safesearch is turned on. This filters explicit images and terms.

Links or feeds to e-safety websites are provided as is other information on the computer home screens to enable children to access support if needed.

CEOP (Child Exploitation and Online Protection Centre) training for Forms IV to VI is annual and part of the PSHEE and Computer curriculum in addition to Gooseberry Planet resources for raising awareness on staying safe and being responsible. A link to the www.thinkukknow.co.uk website is part of the computer's screen layout for further advice and information on children or young people's personal online spaces. Encryption codes on wireless systems prevent hacking.

Parents – Roles

There is no statutory requirement for parents to sign acceptable use policies, but evidence shows that children signing agreements, to take responsibility for their own actions, is successful. For day children, these agreements were signed at home and countersigned by parents so they are aware of the commitments that children have made. These are signed from age 7 upwards as any internet use before this age is on designated websites in lessons only.

Each child or young person should receive a copy of the Acceptable Use Agreement on an annual basis or first-time entry to Barnardiston which needs to be read with the parent, signed and returned to School, confirming both an understanding and acceptance of the agreement. Both child and parent are requested to sign this.

It is expected that parents will explain and discuss the agreement with their child, so that they are clearly understood and accepted.

The School keeps a record of the signed forms.

Support for, and support from, parents

As a part of Barnardiston's commitment to developing e-safety awareness with children, the School may offer parents the opportunity to find out more about how they can support the School in keeping their child safe on line and to find out what they can do to continue to keep them safe whilst using online technologies beyond School. We aim to promote a positive attitude to using the World Wide Web and, therefore, want parents to support their child's learning and understanding of how to use online technologies safely and responsibly.

School will do this by holding an e-safety Parent Information Evening annually and/or providing online seminars for parents to attend, provided by Gooseberry Planet. Part of this evening will provide parents with information on how the School protects children whilst using the learning platform facilities, such as the Internet and e-mail. It will also be an opportunity to explore how the School is teaching children to be safe and responsible Internet users and how this can be extended to use beyond the School for enjoyment.

Curriculum Development

The teaching and learning of e-Safety should be embedded within the School curriculum to ensure that the key safety messages about engaging with people are the same whether children are on or off line. This forms part of the PHSEE module but is not exclusive to this area of curriculum and opportunities to embed e-Safety throughout the curriculum are sought, especially in computing lessons with every year group.

CCTV

To comply with both the General Data Protection Regulations and the Information Commissioner's CCTV Code of Practice, we declare CCTV for security and safety purposes. Barnardiston ensures that all images recorded through the CCTV system are fully traceable with the date, time.

A robust and thoughtful collection of Standard Operating Procedures are in place to govern the day to day operation of the CCTV system. For data security purposes, a restricted number of staff should have access to any images and recordings held by the School.**Fig 1: e-Safety Flow Chart**

Barnardiston Hall Preparatory School

Acceptable Use Agreement for Staff Volunteers and Visitors.

This agreement applies to all online use and to anything that may be downloaded or printed.

All adults within the School must be aware of their safeguarding responsibilities when using any online technologies, such as the internet, E-mail or social networking sites. They are asked to sign this Acceptable Use Agreement so that they provide an example to children for the safe and responsible use of online technologies. This will educate, inform and protect adults so that they feel safeguarded from any potential allegations or inadvertent misuse themselves.

- I know that I must only use the School equipment in an appropriate manner and for professional uses.
- I understand that I need to give permission to children before they can upload images (video or photographs) to the internet or send them via e-mail.
- I know that images should not be inappropriate or reveal any personal information of children if uploading to the internet.
- I have read the Procedures for Incidents of Misuse so that I can effectively deal with any problems that may arise.
- I will report accidental misuse.
- I will report any incidents of concern for a child or young person's safety to the Safeguarding Designated Lead and / or e-Safety Lead.
- I know who my Safeguarding Designated Lead is.
- I know that I am putting myself at risk of misinterpretation and allegation should I contact children via personal technologies, including my personal e-mail. I know I should use the School e-mail address and phones (if provided) and only to a child's School e-mail address as a result of agreed use within the School.
- I know that I must not use the School system for personal use unless this has been agreed by the Headmaster and/or e-Safety Lead.
- I know that I should complete virus checks on my laptop and memory stick or other devices so that I do not inadvertently transfer viruses, especially where I have downloaded resources.
- I will ensure that I follow the Data Protection Act 1998 and I have checked what this involves.

- I will ensure that I keep my password secure and will not disclose any security information unless to appropriate personnel. If I feel someone inappropriate requests my password, I will check with the e-Safety Lead prior to sharing this information.
- I will adhere to copyright and intellectual property rights.
- I will only install hardware and software for which I have been given permission.
- I accept that the use of any technology designed to avoid or bypass the School filtering system is forbidden. I understand that intentional violation of this rule may result in disciplinary procedures being initiated.
- I have been given a copy of the E-Safety Policy to refer to about all e-safety issues and procedures that I should follow.

I have read, understood and agree all the conditions of this Agreement as I know that, by following them, I have a better understanding of e-Safety and my responsibilities to safeguard children when using online technologies.

Signed…… Date……. (Print name:……)

Barnardiston Hall Preparatory School

My e-Safety Agreement for using the internet safely and responsibly.

- I will use the internet to help me to learn.
- I will learn how to use the internet safely and responsibly.
- I will only send e-mail messages that are polite and friendly.
- I will only e-mail, chat to or video-conference people I know in the real world or that a trusted adult has approved.
- Adults are aware when I use online tools such as video-conferencing.
- I agree never to give out passwords or personal information, like my full name, address or phone numbers.
- I agree never to post photographs or video clips without permission and that I will not include my full name with photographs.
- If I need help, I know who I can ask and that I can go to www.thinkuknow.co.uk for help if I cannot talk to a trusted adult.
- If I see anything on the internet that makes me feel uncomfortable, I will tell my parents, whoever is looking after me, and / or Mrs Dobson or another member of staff in School. I understand that it is important to tell someone and I won't get into trouble for reporting something which I did not intend to do. This will help to protect other people in School.
- If I receive a message sent by someone I don't know, I will tell my parents, whoever is looking after me, and / or Mrs Dobson or another member of staff in School
- I know I should follow these guidelines as part of the agreement with my parent/carer/School.
- I agree to look after myself and others by using my internet in a safe and responsible way.

Signed..... Dated.....

Name.....(Printed)

Parents are asked to sign to confirm they have gone through this with their child.

Signature of parent: _____ Date:_____