Dame Ellen Pinsent School
E-Safety and Computing Policy

<table>
<thead>
<tr>
<th>Last Review:</th>
<th>November 2017</th>
<th>S Hammersley</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current Review</td>
<td>March 2019</td>
<td>R Marshall</td>
</tr>
<tr>
<td>Ratified by Governors</td>
<td></td>
<td></td>
</tr>
<tr>
<td>To be Reviewed</td>
<td>March 2021</td>
<td>R Marshall</td>
</tr>
</tbody>
</table>
Development / Monitoring / Review of this Policy

This policy has been reviewed and updated by a working group made up of:

- Assistant Headteacher & Designated Safeguarding Lead (DSL)
- Computing and Technology Coordinator
- E-Safety Committee

Schedule for Development / Monitoring / Review

<table>
<thead>
<tr>
<th>This policy was approved by the Governing Body on:</th>
<th>November 2017</th>
</tr>
</thead>
<tbody>
<tr>
<td>The implementation of this policy will be monitored by the:</td>
<td>DSL, Computing and Technology Coordinator, E-Safety governor, Senior Leadership Team</td>
</tr>
<tr>
<td>Monitoring will take place at regular intervals:</td>
<td>Annually</td>
</tr>
<tr>
<td>The Governing Body will receive a report on the implementation of the e-safety policy (which will include anonymous details of e-safety incidents) at regular intervals:</td>
<td>Annually</td>
</tr>
<tr>
<td>The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be:</td>
<td>November 2018</td>
</tr>
<tr>
<td>Should serious e-safety incidents take place, the following external persons / agencies should be informed:</td>
<td>DSL, Computing and Technology Coordinator, Headteacher, Police, Social Services, Link 2 ICT</td>
</tr>
</tbody>
</table>

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited)
- Internal monitoring data for network activity
- Surveys / questionnaires of
  - students / pupils
  - parents / carers
  - staff

Scope of the Policy

This policy applies to all members of the school community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of the school.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school.
The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

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. A member of the Governing Body has taken on the role of E-Safety Governor. The role of the E-Safety Governor will include:

- regular meetings with the DSL
- regular monitoring of e-safety incident logs
- reporting to relevant Governors meeting

Headteacher and Senior Leaders:

- The Headteacher has a duty of care for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the DSL.
- The Headteacher and (at least) another member of the Senior Leadership Team / Senior Management Team 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 Headteacher / Senior Leaders are responsible for ensuring that the DSL and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The Headteacher / Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

Designated Safeguarding Lead (DSL):

- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- ensures (with SLT and Computing Coordinator) that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- liaises with Local Authority
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- attends relevant meeting / committee of Governors
- meets regularly with E-Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- should be trained in e-safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:
  - sharing of personal data
  - access to illegal / inappropriate materials
  - inappropriate on-line contact with adults / strangers
  - potential or actual incidents of grooming
cyber-bullying

Computing and Technology Coordinator:
- provides training and advice for staff
- receives reports of e-safety incidents and reviews the log of incidents to inform future e-safety developments
- liaises with relevant bodies (e.g. Link2ICT)
- liaises with school technical staff
- meets termly with E-Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- meets regularly with Senior Leadership Team

Network Manager / Technical staff:
The Network Manager for ICT / Computing is responsible for ensuring:
- that the school’s technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required e-safety technical requirements and any Local Authority / other relevant body E-Safety Policy / Guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy.
- that the use of the network / internet / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher for investigation / action / sanction
- That monitoring software is implemented and updated as agreed by the school

Teaching and Support Staff
are responsible for ensuring that:
- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem to the Headteacher / Computing Coordinator / DSL for investigation / action / sanction
- all digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official school systems
- e-safety issues are embedded in all aspects of the curriculum and other activities
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- No child will use the internet without a teacher or responsible adult giving permission and being present, ensuring that all use is being carefully monitored.

E-Safety Committee
The E-Safety Committee provides a consultative group that has wide representation from the school, with
responsibility for issues regarding e-safety and the monitoring the e-safety policy including the impact of initiatives. The committee will also be responsible for regular reporting to the Governing Body.

Members of the E-safety Committee will assist the DSL and Computing Coordinator with:
- the production / review / monitoring of the school e-safety policy / documents.
- mapping and reviewing the e-safety curricular provision – ensuring relevance, breadth and progression
- monitoring network / internet / incident logs
- consulting stakeholders – including parents / carers and the students / pupils about the e-safety provision
- monitoring improvement actions identified through use of the 360 degree safe self review tool

Students / pupils:

- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know who to go to in school
- should understand the importance of adopting good e-safety practice when using digital technologies out of school.

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents’ evenings, newsletters, letters, website and information about national / local e-safety campaigns / 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
- access to parents’ sections of the website and pupil records

Community Users

Community Users who access school systems / website as part of the wider school provision will be expected to sign a Community User AUA before being provided with access to school systems.

Policy Statements

Education – students / pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating students / pupils to take a responsible approach. The education of students / pupils in e-safety is therefore an essential part of the school’s e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum. The e-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:
- A planned e-safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited
- Key e-safety messages should be reinforced as part of a planned programme of assemblies.
- Students / pupils should be taught in all lessons to be aware of the materials / content they access on-line.
• Students / pupils should be encouraged to adopt safe and responsible use both within and outside school
• Staff should act as good role models in their use of digital technologies, the internet and mobile devices
• In lessons where internet use is pre-planned, it is best practice that students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
• Where students / pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites they visit.
• It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Education – parents / carers
Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children’s on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:
• Curriculum activities on website
• Letters, newsletters, web site
• Parents / Carers evenings / workshops
• High profile events / campaigns eg Safer Internet Day

Education – The Wider Community
The school will provide opportunities for local community groups / members of the community to gain from the school’s e-safety knowledge and experience. This may be offered through the following:
• Providing family learning courses in use of new digital technologies, digital literacy and e-safety.
• E-Safety messages targeted towards grandparents and other relatives as well as parents.
• The school website will provide e-safety information for the wider community (curriculum).

Education & Training – Staff / Volunteers
It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:
• A planned programme of formal e-safety training will be made available to staff. This will be regularly updated and reinforced.
• All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Agreements.
• The E-Safety Coordinator will receive regular updates through attendance at external training events (eg CEOP) and by reviewing guidance documents released by relevant organisations.
• This E-Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / briefings.
• The E-Safety Coordinator / Officer (or other nominated person) will provide advice / guidance / training to individuals as required.

Training – Governors
Governors should take part in e-safety training / awareness sessions, with particular importance for those who are members involved in e-safety / child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association / or other relevant organisation.
- Participation in school training / information sessions for staff or parents.

Technical – infrastructure / equipment, filtering and monitoring

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 in the above sections will be effective in carrying out their e-safety responsibilities:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of school academy technical systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to school technical systems and devices.
- All classes will be provided with a username.
- The “master / administrator” passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the Headteacher or other nominated senior leader and kept in a secure place (eg school safe).
- The network manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.

- Internet access is filtered for all users. Illegal content is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes.
  - School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
  - An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person, as agreed.
  - 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.
  - An agreed policy is in place for the provision of temporary access of “guests” (eg trainee teachers, supply teachers, visitors) onto the school systems.
  - An agreed policy is in place regarding the extent of personal use that users (staff) and their family members are allowed on school devices that may be used out of school.
  - An agreed policy is in place that allows staff to / forbids staff from downloading executable files and installing programmes on school devices.
  - An agreed policy is in place regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students / pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and students / pupils need to be aware of the risks associated with publishing
digital images on the internet. Such images may provide avenues for cyberbullying 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. It is common for employers to carry out internet searches for information about potential and existing employees. 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 students / 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 eg on 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 in not covered by the Data Protection Act). To respect everyone’s privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other students / 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. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
• Care should be taken when taking digital / video images that students / pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
• Students / pupils must not take, use, share, publish or distribute images of others without their permission
• Photographs published on the website, or elsewhere that include students / pupils will be selected carefully and will comply with good practice guidance on the use of such images.
• Students’ / Pupils’ full names will not be used anywhere on a website or blog, particularly in association with photographs.
• Written permission from parents or carers will be obtained before photographs of students / pupils are published on the school website
• Student’s / Pupil’s work can only be published with the permission of the parents or carers.

Social Media - Protecting Professional Identity

All schools, academies and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools/academies and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school / academy or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:

• Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
• Clear reporting guidance, including responsibilities, procedures and sanctions
• Risk assessment, including legal risk

School staff should ensure that:

• No reference should be made in social media to students / pupils, parents / carers or school staff
• They do not engage in online discussion on personal matters relating to members of the school community
• Personal opinions should not be attributed to the school
• Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.
The school's use of social media for professional purposes will be checked regularly by the senior risk officer and e-safety committee to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies.

Unsuitable / inappropriate activities
The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts usage as follows:

<table>
<thead>
<tr>
<th>User Actions</th>
<th>Acceptable</th>
<th>Acceptable at certain times</th>
<th>Acceptable for nominated users</th>
<th>Unacceptable</th>
<th>Unacceptable and illegal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>- Child sexual abuse images --The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>- Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>- Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>- Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>- Pornography</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>- Promotion of any kind of discrimination</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>- Threatening behaviour, including promotion of physical violence or mental harm</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>- Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Using school systems to run a private business</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Infringing copyright</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Creating or propagating computer viruses or other harmful files</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unfair usage (downloading / uploading large files that hinders others in their use of the internet)</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Responding to incidents of misuse
This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see “User Actions” above).

Illegal Incidents
If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.
Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school / academy 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 the event of suspicion, all steps in this procedure should be followed:
- Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the url of any site containing the alleged misuse and describe 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 – see below).
Once this has been completed and fully investigated 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 the following:

- Internal response or discipline procedures
- Involvement by Local Authority or national / local organisation (as relevant).
- Police involvement and/or action

If content being reviewed includes images of Child abuse then the monitoring should 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

Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the school / academy and possibly the police and 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.

**School Actions & Sanctions**

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures (see relevant policies).
AIMS

- Computing can motivate and enthuse pupils; it should be fun.
- Computing promotes access to otherwise inaccessible areas of the curriculum.
- Computing can present information in new ways which help students to understand, assimilate and use it more readily.
- Computing develops skills in decision making, cause and effect, and understanding the elements of control.
- Computing should help children to focus and concentrate.
- All children regardless of ability, age, gender or race will have appropriate and equal access to Computing
- Appropriate technologies will be provided to enable all pupils to achieve full access to the curriculum and the life of the school (see examples below)

WHAT DOES COMPUTING COVER?

As well as being an important national curriculum requirement, the ability to use Computing effectively is a vital life skill in modern society. We interpret Computing to include the use of any equipment which allows users to communicate or manipulate information (in the broadest sense of the word) electronically. This includes use of:

- Computers
- iPads
- interactive whiteboards, projectors and touch screens
- touch table computers
- programmable toys and control kits e.g. Beebots, remote control toys
- assistive technology, e.g. switch toys
- sensors and probes such as light and sound sensors.
- electronic musical instruments, including Skoog 2.0
- audio and video recorders
- the Internet

CURRICULUM ORGANISATION

- All teachers are encouraged to use Computing (including iPads) where appropriate and include this in their planning. The Computing coordinator ensures that teachers have a wide variety of software and apps for iPads (suitable for the curricular areas and the pupils). Training has, and will continue to be, provided, by the Computing Coordinator, for teachers and support staff to improve their Computing and iPad skills.
- All pupils have access to iPads with 1:1 iPads in Key Stage Two.
• Use of iPads will be class based and integrated as part of normal class based activity. It will include individual, paired, small group and class-based activities. All classrooms are equipped with computers (with Air Server), interactive whiteboards or touch screens. In addition an Apple TV and two iMacs are available in the Computing Room.

• Assessment of Computing will be at the discretion of each class teacher using the following criteria: degree of interest shown by pupils; confidence; range of software (apps) with which they are familiar and which they can use competently.

• Computing shall be taught through other subjects, as far as possible. Guidance as to activities taught within units and link these to outcome and assessment opportunities is available for many units in Topics and Science.

• A Computing scheme of work was put in place during 2015. It is based on a two year rolling program. It is expected that 1 lesson each week will be taught from this scheme in order to increase the children’s discrete ICT skills.

• Teachers are encouraged to use the iPads to assist with children’s learning. If additional apps are required the teachers are required to ask the Computing Coordinator to purchase and apply this app to the appropriate set of iPads.

ROLES AND RESPONSIBILITIES

Responsibilities of computing coordinator.
• Advise on the training and support for whole staff and individual teachers
• Liaise with Curriculum Coordinators to ensure that computing is included in school policies and schemes of work for the various curriculum areas.
• To monitor the above
• The computing coordinator to hold an inventory of computers and peripherals, software licenses, serial numbers and approximate purchase date.
• Maintain a coordinating role in the purchase of suitable hardware and software and maintain inventory including licenses.
• Support other teachers in the use and development of computing in the curriculum

Responsibilities of class teachers
• Integrate computing throughout curriculum
• To give training in the safe use of the internet as appropriate to the children’s needs (E-safety)
• Assessment of pupils’ skills. It is important that individual records are updated on a regular basis (minimum October, February, May) and that this assessment is used to ensure appropriate target setting.
• To keep coordinator informed of the use of computing within the classroom.
• To provide material for class web page every half term.
• Where appropriate to follow up training provided with activities in class.

Responsibilities of Curriculum Coordinators
• To have an overview of the possible uses of computing within their subject.
• To make suggestions to add to the computing scheme of work.
• To support staff in the use of computing within their curriculum area.

PROFESSIONAL DEVELOPMENT

TECHNICAL SUPPORT

A technician is employed one and a half days per week.
RESOURCES
- At present computing is well resourced within our school.
- There are 136 iPads available for children to use with 1:1 rollout in all key stage two classes. A Macbook Pro is kept with the iPads in order to update and configure them.
- All classrooms are equipped with interactive boards/screens
- The Reception class is equipped with a touch table computer.
- In addition an Apple TV and two iMacs are available in the Computing Room.
- All SLT, teachers and HLTA’s have been issued with an appropriate laptop and iPad to be used for planning and working from home. In addition, there are 3 ‘floating’ iPads for other staff to use at the discretion of the Computing Coordinator.
- Currently our computing needs are met within the school budget
- Needs are identified by reviewing current status and discussion with teachers.
- It is necessary to maintain a development goal including updating of hardware, software and peripherals.

SOFTWARE
- A good selection of subject specific and open ended use software is available on the school network.
- The school has subscribed to a variety of on line providers – Education City, Help Kidz Learn, Ten Town, See Saw, Twinkl and School Bus.

ACCESS TO INTERNET
- Internet access is available in every classroom, the library, staffroom, technology room and all offices. There is also a full secure wireless network that can be accessed in line with Internet usage agreements.

WEB PAGE
- The web page is maintained by the Assistant Headteacher in liaison with Primary Suite. Teachers are responsible for providing the content for their own class page, as are subject coordinators; this should be updated in a timely fashion.
- The web page will provide information to parents on current news and dates, curriculum information, specialist resources, the opportunity to view and celebrate children’s achievement. All parents will be asked for written permission to put photos of their child on the website.
Acceptable Use of the Internet Policy
Dame Ellen Pinsent School

I have received and read a copy of the above Policy and agree to follow the guidelines set out in this Policy.

Name  _______________________________________________________

Position  ________________________________

Date  __________________________

Please sign and return to office ASAP
AUP Guidelines for any adult working with learners

I agree that I will:

- only use, move and share personal data securely
- respect the school network security
- implement the schools policy on the use of technology and digital literacy including the skills of knowledge location, retrieval and evaluation, the recognition of bias, unreliability and validity of sources
- respect the copyright and intellectual property rights of others
- only use approved email accounts
- only use pupil images or work when approved by parents and in a way that will not enable individual pupils to be identified on a public facing site.
- only give permission to pupils to communicate online with trusted users.
- use the Computing facilities sensibly, professionally, lawfully, consistent with my duties and with respect for pupils and colleagues.
- not use or share my personal (home) accounts/data (eg Facebook, email, ebay etc) with pupils
- set strong passwords which I will not share and will change regularly (a strong password is one which uses a combination of letters, numbers and other permitted signs).
- report unsuitable content and/or Computing misuse to the named e-Safety officer
- promote any supplied E-safety guidance appropriately.

I know that anything I share online may be monitored.
I know that once I share anything online it is completely out of my control and may be used by others in a way that I did not intend.

Continued…
I agree that I will not:

- visit Internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:
  - pornography (including child pornography)
  - promoting discrimination of any kind
  - promoting violence or bullying
  - promoting racial or religious hatred
  - promoting illegal acts
  - breach any Local Authority/School policies, e.g. gambling
  - do anything which exposes others to danger
  - any other information which may be offensive to others
  - forward chain letters
  - breach copyright law
  - use personal digital recording equipment including cameras, phones or other devices for taking/transferring images of pupils or staff without permission
  - store images or other files off site without permission from the head teacher or their delegated representative.

I will ensure that any private social networking sites, blogs, etc that I create or actively contribute to, do not compromise my professional role.

I understand that data protection policy requires me to keep any information I see regarding staff or pupils which is held within the school’s management information system private, secure and confidential. The only exceptions are when there is a safeguarding issue or I am required by law to disclose such information to an appropriate authority.

I accept that my use of the school and Local Authority Computing facilities may be monitored and the outcomes of the monitoring may be used.
AUP Guidelines for Governors

The governors will ensure that:

- learners are encouraged to enjoy the safe use of digital technology to enrich their learning
- learners are made aware of risks and processes for safe digital use
- all adults and learners have received the appropriate acceptable use policies and any required training
- the school has appointed an e-Safety Coordinator and a named governor takes responsibility for e-Safety
- an e-Safety Policy has been written by the school, building on the LSCB e Safety Policy and BECTA guidance
- the e-Safety Policy and its implementation will be reviewed annually
- the school internet access is designed for educational use and will include appropriate filtering and monitoring
- copyright law is not breached
- learners are taught to evaluate digital materials appropriately
- parents are aware of the acceptable use policy
- parents will be informed that all technology usage may be subject to monitoring, including URL’s and text
- the school will take all reasonable precautions to ensure that users access only appropriate material
- the school will audit use of technology (using the Self-Review Framework) to establish if the e-safety policy is adequate and appropriately implemented
- methods to identify, assess and minimise risks will be reviewed annually
- complaints of internet misuse will be dealt with by a senior member of staff
Data Protection Policy

1 The school will comply with:

1.1 The terms of the 1998 Data Protection Act, and any subsequent relevant legislation, to ensure personal data is treated in a manner that is fair and lawful.

1.2 Birmingham Education Service advice and guidance supplied in the Data Protection Advice for Schools flyer and Data Protection Guidance for Schools booklet.

1.3 Information and guidance displayed on the Information Commissioner’s website (www.dataprotection.gov.uk).

2 This policy should be used in conjunction with the school’s Internet Use Policy.

3 Data Gathering

3.1 All personal data relating to staff, pupils or other people with whom we have contact, whether held on computer or in paper files, are covered by the Act.

3.2 Only relevant personal data may be collected and the person from whom it is collected should be informed of the data’s intended use and any possible disclosures of the information that may be made.

4 Data Storage

4.1 Personal data will be stored in a secure and safe manner.

4.2 Electronic data will be protected by standard password and firewall systems operated by the school.

4.3 Computer workstations in administrative areas will be positioned so that they are not visible to casual observers waiting either in the office or at the reception hatch.

4.4 Manual data will be stored where it not accessible to anyone who does not have a legitimate reason to view or process that data.

4.5 Particular attention will be paid to the need for security of sensitive personal data.

5 Data Checking

5.1 The school will issue regular reminders to staff and parents to ensure that personal data held is up-to-date and accurate.

5.2 Any errors discovered would be rectified and, if the incorrect information has been disclosed to a third party, any recipients informed of the corrected data.

6. Form Statements
In order to ensure that processing of personal information is considered to be fair and lawful (meeting the set conditions within Schedule 2 of the Act), the school, in its role as data controller, will ensure that the data subject has been provided with the following:

6.1 That the identity of the data controller is clear; i.e. the name of the school is specified.
6.2 The purpose for which the data is intended to be processed. Quite often, this information may be contained within the title of a form, but if it is not obvious it should be stated.
6.3 Any consequences of such processing which are not obvious to the data subject, and;
6.4 Any envisaged disclosures which are not obvious to the data subject

In order to meet points 2 - 4 as listed above, a Data Protection Statement is often required. This statement must not appear in a smaller font than that used for the majority of the form. The statement should ideally appear on the top of the form so that the data subject is made aware of the implications of their data being processed before they start to complete the form.

7 Data Disclosures

Personal information can only be disclosed:

1. to the data subject (the person to whom the data relates);
2. with the data subject’s consent;
3. if required in life and death situations (Schedule 2 of the Act);
4. if it is covered by an exemption;
5. if it is to a notified recipient (a registered disclosure). This would be detailed in the Notification of Personal Data form for automated data; or
6. if the disclosure is necessary to carry out the purpose for which the personal data has been obtained fairly and lawfully (note: the data subject should be aware of such disclosures).

If the school needs to disclose an individual’s information to deal with an enquiry one of points 1 – 6 above should apply. If the school are at all unsure about making a disclosure, the individual involved will take the individual’s telephone number and speak with their line manager. If there are any remaining doubts about disclosing personal data, the school will liaise with the Education Service Data Protection Officer before making the disclosure.

7.1 Personal data will only be disclosed to organisations or individuals for whom consent has been given to receive the data, or organizations that have a legal right to receive the data without consent being given.

7.2 When requests to disclose personal data are received by telephone it is the responsibility of the school to ensure the caller is entitled to receive the data and that they are who they say they are. It is advisable to call them back, preferably via a switchboard, to ensure the possibility of fraud is minimised.

7.3 If a personal request is made for personal data to be disclosed it is again the responsibility of the school to ensure the caller is entitled to receive the data and that
they are who they say they are. If the person is not known personally, proof of identity should be requested.

7.4 Personal data will not be used in newsletters, websites or other media without the consent of the data subject.

7.5 Routine consent issues will be incorporated into the school’s pupil data gathering sheets, to avoid the need for frequent, similar requests for consent being made by the school.

7.6 Personal data will only be disclosed to Police Officers if they are able to supply a WA170 form which notifies of a specific, legitimate need to have access to specific personal data. This form is the agreed procedure between Birmingham City Council and West Midlands Police.

7.7 A record should be kept of any personal data disclosed so that the recipient can be informed if the data is later found to be inaccurate.

8 Subject Access Requests

8.1 If the school receives a written request from a data subject to see any or all personal data that the school holds about them this should be treated as a Subject Access Request and the school will respond within the 40 day deadline.

8.2 Informal requests to view or have copies or personal data will be dealt with wherever possible at a mutually convenient time but, in the event of any disagreement over this, the person requesting the data will be instructed to make their application in writing and the school will comply with its duty to respond within the 40 day time limit.

9. This policy will be included in the Staff Handbook.

10. Data Protection statements will be included in the school prospectus and on any forms that are used to collect personal data.

Appendices
- Pupil data gathering sheets/covering letter
- Pupil data checking sheet/covering letter
- Staff data gathering sheets/covering letter
- Reception initial enquiry data gathering sheet
- School transfer initial enquiry data gathering sheet
Computing Health and Safety Policy

Richard Marshall

**General Environment**

**Comfort**
Users should be comfortably positioned, with easy access to all equipment. Whilst sitting, it is essential that the user can adjust his or her position in relation to the equipment as appropriate. Users should take frequent short breaks from computer work.

**Space**
There should be enough space around a workstation for paper, books and any other materials, including special educational needs equipment such as concept keyboards. There should also be space for more than one pupil at a time, and for the teacher to gain access. It is important to ensure that gangways and emergency exits are kept clear.

**Noise**
Almost all Computing equipment emits background noise if the power is switched on, even when not in use. Many software packages also feature sound as part of their operation.
Other users can be noisy or distracting, especially those working in groups. Headphones will help to reduce distractions and aid concentration.

**Heat and light**
Ideally, the temperature of a Computing suite should be between 18° and 24° degrees, with humidity between 40 per cent and 60 per cent. Almost all Computing equipment gives off heat which can build up during the day and be quite oppressive for users, as well as detrimental to the equipment.
Ensure that the room is well ventilated. Blinds/curtains should be used to ensure that users do not suffer from glare. Screens should be regularly cleaned.

**Seating**
Seating in the classrooms is correctly sized for the children who are using it and to make working at the built in workstations comfortable. It is not practical nor safe to have wheeled computer chairs in many of the classrooms or Computing Suite.
Users should change posture frequently and take 10-minute breaks away from the computer to stretch their limbs.

**Using the Computing equipment**

**Monitors**
These should tilt and swivel to suit the requirements of individual users. Screens should be positioned to reduce reflections and glare from lights and windows. The top of the screen should be roughly at eye level.
There is a slight risk of triggering epileptic seizures from excessive screen flicker – there
is wide variation in the ‘steadiness’ of screen image from one monitor to another. If an individual child is at risk then consult with the relevant therapist or doctor when choosing a screen for them to use. All pupils should have regular eye check-ups.

**Keyboards**
Users should have the option to have the keyboard flat or tilted. It is important to develop a good keyboard technique.

**Mice**
Show pupils how to hold the mouse lightly in the widest part of the hand with their fingers resting lightly on the mouse button(s) so that a very small movement is needed to click a button. A small mouse is best for those with small hands. The arm or wrist should be supported on the table or wrist rest and check that they don’t extend one or more fingers stiffly as this can lead to muscle strain.

**Interactive white boards**
When using an interactive whiteboard, make sure that children are supervised at all times during the projector’s operation. Users should never stare directly into the beam of the projector, and when entering the beam, should not look towards the audience, or class, for more than a few seconds. If possible users should keep their backs to the beam at all times, and factors such as positioning should be given careful consideration. It is generally viewed that a maximum of 1500 ANSI lumens is adequate for projection equipment in most classroom environments, except in the most extreme ambient lighting conditions, where it is advised that window blinds are used rather than increasing the brightness of the projector.

**Software**
Software should be easy to use and appropriate for the task. Sound may be an issue on some software, and if necessary, headphones should be used.
Using defective CD-ROMs or DVDs in high-speed drives can cause them to shatter and lead to pieces of disk escaping from the drive. To ensure that disks are in perfect condition, hold them up to the light to check for cracks, scratches or defects near the inner rim.

**Electrical safety**
Under the Electricity at Work Regulations Act 1989, all electrical equipment should be maintained regularly (PAT testing). Always leave technical repairs to the experts. Ensure that you have the necessary carbon dioxide fire extinguishers positioned near any Computing equipment. The location of electrical equipment depends on the length of cables and the availability of sockets for telephones, TV aerials and power. It is essential that the location of the equipment does not increase the risk of danger to equipment or users. The school should ensure that there is a system in place for regular visual checks of plugs, leads and other electrical equipment.

Check regularly to make sure the computer equipment is sitting in a stable position and hasn't been pushed or tilted too far. Don't use the top of the computer or monitor as a storage shelf as you may block ventilation grills and cause overheating.
Promoting good health and safety practice for pupils

Pupils should take a break from the computer at least once every twenty minutes, and should do some simple stretching exercises to relieve the muscles they have been using, for example their hands, wrists and neck. It's a good idea to get up and walk around at least once an hour, although obviously this would need to be well managed in a classroom environment. Eye muscles should be refreshed by looking at distant objects as well as those close up. Pupils can be encouraged to make these exercises into their own personal ‘computer workout’ routine.

Posture is also very important and pupils should be given a few simple guidelines. Make sure they are not constantly leaning their head forward (it is very heavy for the neck to support!), and encourage them to keep the chin tucked in. The back should be supported in an upright position in the chair and the body should face forwards, not twisted sideways.

Pupils sharing a computer should be encouraged to make sure that everyone in the group can see without straining.

Meeting the requirements of the Special Education Needs Disability Act (SENDA) 2002

All children regardless of ability, age, gender or race will have appropriate and equal access to Computing

Appropriate technologies will be provided to enable all pupils to achieve full access to the curriculum and the life of the school
Internet Access Policy

RATIONALE
Providing access to the internet in school contributes towards the raising of standards and supports the professional work of staff

CONTEXT
This policy outlines our purpose in providing e-mail facilities and access to the Internet at (insert name) and explains how the school is seeking to avoid the potential problems that unrestricted internet access could give rise to.

INTERNET ACCESS IN SCHOOL
Staff and pupils have access to web sites worldwide offering educational resources, news and current events. There will be opportunities for discussion and exchange of information within the school community and others worldwide.

Staff have the opportunity to access educational materials and good curriculum practice, to communicate with the advisory and support services, professional associations and colleagues; exchange curriculum and administration data with the Local Authority and Department for Education and Skills (DfES); receive up-to-date information and participate in government initiatives such as National Grid for Learning (NGfL) and the Virtual Teacher Centre.

The internet is also be used to enhance the school’s management information and business administration systems.

Staff, including supply staff, will not be expected to take charge of an internet activity without training. Staff should be given opportunities to discuss the issues and develop good teaching strategies. All staff (including teachers, supply staff and classroom assistants) and any other adults involved in supervising children accessing the internet, will be provided with the School Internet Access Policy, and will have its importance explained to them.

Parents’ attention will be drawn to the Policy and will be available for parents and others to read on request.

ENSURING INTERNET ACCESS IS APPROPRIATE AND SAFE
The internet is freely available to any person wishing to send e-mail or publish a web site and therefore some material available on the internet is unsuitable for children. The following key measures have been adopted to help ensure that our pupils are not exposed to unsuitable material:

- Our internet access is managed by the Local Authority, which provides a service designed for pupils including a "firewall" filtering system intended to prevent access to material inappropriate for children;

- Children using the internet will normally be working in the classroom, during lesson time and will be supervised by an adult (usually the class teacher) at all times;

- Staff will check that the sites pre-selected for pupil use are appropriate to the age and maturity of pupils;

- Staff will be particularly vigilant when pupils are undertaking their own search and will check that the children are following the agreed search plan;

- Pupils will be taught to use e-mail and the internet responsibly in order to reduce the risk to themselves and others;

- The Computing co-ordinator will monitor the effectiveness of internet access strategies;
- The Computing co-ordinator/network manager will ensure that occasional checks are made on files to monitor compliance with the school's Internet Access Policy;

- The headteacher will ensure that the policy is implemented effectively;

- Methods to quantify and minimise the risk of pupils being exposed to inappropriate material will be reviewed in consultation with colleagues and advice from the Local Authority;

- Pupils will be taught to tell a teacher immediately if they encounter any material that makes them feel uncomfortable.

- If there is an incident in which a pupil is exposed to offensive or upsetting material the school will wish to respond to the situation quickly and on a number of levels. Responsibility for handing incidents involving children will be taken by the Computing Co-ordinator and the Child Protection Officer in consultation with the Head Teacher and the pupil's class teacher. All the teaching staff will be made aware of the incident in Pupil Awareness at a Staff Meeting if appropriate.

- If one or more pupils discover (view) inappropriate material our first priority will be to give them appropriate support. The pupil's parents/carers will be informed and given an explanation of the course of action the school has taken. The school aims to work with parents/carers and pupils to resolve any issue;

- If staff or pupils discover unsuitable sites the Computing co-ordinator will be informed. The Computing co-ordinator will report the URL (address) and content to the Internet Service Provider and the Local Authority (Link 2 ICT). If it is thought that the material is illegal, after consultation with the Local Authority, the site will be referred to the Internet Watch Foundation and the police.

- Pupils are expected to play their part in reducing the risk of viewing inappropriate material by obeying the Rules of Responsible Internet Use, which have been designed to help protect them from exposure to internet sites carrying offensive material. If pupils abuse the privileges of access to the internet or use of e-mail facilities by failing to follow the rules they have been taught or failing to follow the agreed search plan when given the privilege of undertaking their own internet search, then sanctions consistent with our School Behaviour Policy will be applied. This may involve informing the parents/carers. Teachers may also consider whether access to the internet may be denied for a period.

**MAINTAINING SECURITY**

We are aware that connection to the internet significantly increases the risk that a computer or a computer network may be infected by a virus or accessed by unauthorised persons.

The Computing Technician/Network Manager will up-date virus protection regularly. The Computing co-ordinator will keep up-to-date with Computing news developments and work with the LEA and Internet Service Provider to ensure system security strategies to protect the integrity of the network are reviewed regularly and improved as and when necessary.

**USING THE INTERNET TO ENHANCE LEARNING**

Pupils will learn how to use a web browser. Older pupils will be taught to use suitable web search engines. Staff and pupils will begin to use the internet to find and evaluate information. Access to the internet will become a planned part of the curriculum that will enrich and extend learning activities and will be integrated into the class schemes of work.

As in other areas of their work, we recognise that pupils learn most effectively when they are given clear objectives for internet use.

Different ways of accessing information from the internet will be used depending upon the nature of the material being accessed and the age of the pupils:

- Access to the internet may be by teacher (or sometimes other-adult) demonstration;
• Pupils may access teacher-prepared materials, rather than the open internet;
• Pupils may be given a suitable web page or a single web site to access;
• Pupils may be provided with lists of relevant and suitable web site which they may access;
• Pupils accessing the internet will be supervised by an adult, normally their teacher, at all times.

USING INFORMATION FROM THE INTERNET
In order to use information from the internet effectively, Computing is important for pupils to develop an understanding of the nature of the internet and the information available on Computing. In particular, they should know that most of the information on the internet is intended for an adult audience, much of the information on the internet is not properly audited/edited and most of Computing is copyright.

Staff will ensure that pupils are aware of the need to validate information whenever possible before accepting Computing as true, and understand that this is even more important when considering information from the internet (as a non-moderated medium).

- When copying materials from the Web, pupils will be taught to observe copyright.

Pupils will be made aware that the writer of an e-mail or the author of a web page may not be the person claimed.

USING EMAIL
It is important that communications with persons and organisations are properly managed to ensure appropriate educational use and that the good name of the school is maintained. Therefore:

• Pupils will only be allowed to use e-mail once they have been taught the Rules of Responsible Internet Use and the reasons for these rules.
• Staff will endeavour to ensure that these rules remain uppermost in the children's minds as they monitor children using e-mail;
• Pupils may send e-mail as part of planned lessons but will not be given individual e-mail accounts at present;
• In-coming e-mail to pupils will not be regarded as private;
• Pupils will have the e-mail messages they compose checked by a member of staff before sending them;
• The forwarding of chain letters will not be permitted;
• Pupils will not be permitted to use e-mail at school to arrange to meet someone outside school hours.

THE SCHOOL WEBSITE
Our school web site is intended to:

• Provide accurate, up-to-date information about our school;
• Enable pupils to publish work to a high standard, for a very wide audience including pupils, parents, staff, governors, members of the local community and others;
• Celebrate good work;
• Provide pupils with the opportunity to publish their work on the internet;
Promote the school.

All classes may provide work for publication on the school web site. Staff will be responsible for ensuring that the content of the pupils’ work is accurate and the quality of presentation is maintained. All material must be the author's own work, crediting other work included and stating clearly that author's identity and/or status. The class teacher/subject co-ordinators are responsible for up-loading pages to the school web site, ensuring that the links work and are up-to-date, and that the site meets the requirements of the site host.

The point of contact on the web site will be the school address, telephone number and e-mail address. We do not publish pupils’ full names that identify individuals on our web pages. Home information or individual e-mail identities will not be published. Staff will be identified by their title and surname unless they request otherwise. Permission will be sought from other individuals before they are referred to by name on any pages we publish on our web site.

INTERNET ACCESS AND HOME/SCHOOL LINKS
Parents will be informed that pupils are provided with supervised internet access as part of their lessons. We will keep parents in touch with future Computing developments by letter and newsletter.

School and Local Authority guidelines on issues such as safe internet use will be made available to parents together with printed information and internet sites providing information for parents about safe access for children;

RULES FOR RESPONSIBLE INTERNET USE
The school has installed computers with internet access to help our learning. These rules will help keep us safe and help us be fair to others. Pupils and Staff will

- Only access the computer system with the login and password they have been given;
- Will not access other people's files;
- Will not bring in CDs from outside school and try to use them on the school computers.
- Will report any unpleasant material immediately
- Understand that the school may check my computer files and may monitor the internet visited;
- Will immediately report any unpleasant messages sent
- Understand that e-mail messages received may be read by others.

Date agreed by the Governing Body:

Signed: (see original document)