Parsons Down Partnership of Schools
E-Safety Policy
April 2014

E-safety is a crucial area in protecting the wellbeing of the children across our Partnership as children are becoming more computer literate at younger ages. Technology offers unimaginable opportunities for education, communication and entertainment. Computers, mobile devices and gaming systems are constantly developing how and where children can access different online environments.

We aim to:

★ Develop informed learners who can identify and minimise risks, which may be amplified by technology.
★ Make children aware of their rights and responsibilities when working online so that they understand what makes safe and responsible online behaviour.
★ Educate children so they are clear and confident about how to report their concerns. As a Partnership, to have the appropriate mechanisms to intervene and support any incidents where appropriate.

Responsibility

E-safety provision is therefore a responsibility shared by staff, governors, parents and the pupils themselves.

- Parents: Supervising children during out of school hours; ensuring they are accessing suitable and age appropriate material; monitor use of social networking sites.
- Pupils: Responsible for the choices and decisions they make online when accessing content and communicating with others; adhere to the Acceptable Use Policy; follow the e-safety guidelines they have been taught and report any concerns.
- Staff: Supervise and monitor access whilst children are on site; teach children about responsible use and behaviour in an online environment; report and manage any e-safety incidents.
- ICT subject leader: Manage onsite filtering; monitor the coverage of teaching; provision and maintenance of equipment with support from the ICT Support Assistance.
- Senior Staff: Deal with any incidents of staff or children misuse and issue appropriate sanctions.
- Governors: Ensure a safe environment is provided for the children and monitor any issues which arise and ensure they are effectively dealt with.

Teaching and learning

The Internet is an essential element in 21st century life for education, business and social interaction. The Partnership has a duty to provide children with quality Internet access as part of their learning experience. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation. (See Appendix 3 - Guidelines for teaching E-Safety)

Risk Assessment

The Partnership will take all reasonable precautions to ensure that users access only appropriate material. Our Partnership operates a 'managed' system which provides opportunities for children to learn how to assess and manage risks in a safe environment. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. (See Appendix 1 – Risk Assessment Log) This log will be completed and monitored by the subject leader on an annual basis.

There are three main areas of risk which this policy focuses on covering:

1. Content: being exposed to illegal, inappropriate or harmful material.
2. Contact: being subjected to harmful online interaction with other users.
3. Conduct: personal online behaviour that increases the likelihood of, or causes harm.

Handling e-safety complaints

Complaints of Internet misuse will be dealt with by a senior member of staff. All issues will be logged on an incident sheet and monitored by the ICT subject leader (See Appendix 2 – E-safety Incident Log). Children who do not follow the agreed Acceptable Use Policy will receive appropriate sanctions depending on the incident. Access to the school network or VLE may be removed; instant red cards may be issued for incidents of racism, direct swearing or aggressive behaviour. Any complaint about staff misuse must be referred to the Head of School. Complaints of a child protection/safeguarding nature must be dealt with in accordance with the Partnership Child Protection/Safeguarding procedures (through the Executive Headteacher as designated Child Protection Officer).

Filtering

The Partnership Internet access is designed expressly for pupil use and includes filtering appropriate to the age of pupils. Pupils will be taught what Internet use is acceptable and what is not and give clear objectives for Internet use. Our Partnership operates a 'managed' system which provides opportunities for children to learn how to assess and manage risks in a safe environment. Filtering is monitored and managed within school following LA guidance to ensure systems to protect pupils are reviewed and improved. If staff or pupils discover an unsuitable site, it must be reported to the ICT subject leader. Pupils access is limited by filtering services

however staff have the ability to log in and access a wider range of sites, such as Youtube. Staff must not log children into blocked sites and must ensure they log off fully when leaving a machine.

Managing Network and Internet Access
Partnership ICT systems capacity and security will be reviewed regularly. All staff and pupils will be issued with user log-ons and passwords with differentiated rights and privileges. Sophos antivirus protection is updated regularly on all Partnership machines and laptops.
All pupils and staff with have access to their own personal storage space on the network, as well as access to specific shared drives, which they will be taught to use appropriately.

E-mail
Pupils are able to access their own personal email account through DB Primary. This is a closed email account which only allows them to send and receive emails from other school users. Pupils must immediately tell a teacher if they receive offensive e-mail in person or through the 'whistle blowing tool' on the VLE. Pupils must not reveal personal details of themselves or others in e-mail communication. Staff are issued with a secure Openhive Email Account which they can use in accordance with our Acceptable Use of ICT Policy. This email is also monitored by a filtering policy which may block some emails if their content is considered inappropriate. When appropriate it is possible for the ICT Subject Leader to request CAPITA to release and resend blocked emails to the recipient.

School web site
Our Partnership web site includes the school address, e-mail and telephone number. Staff or pupils' personal information will not be published. The Executive Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate. Photographs of children's work must not show pupils. Pupil's work and images can only be published with the permission of the pupil and parents. Pupils' full names will not be used anywhere on the Web site.

Social networking (please read in conjunction with Social Networking Policy)
The school will block access to social networking sites. Pupils and parents are advised that the use of social network spaces outside school is inappropriate for primary aged pupils. Pupils are able to access a monitored social networking site through the school's Virtual Learning Environment, DB Primary. This is tightly controlled and monitored by staff and is used for the purposes of teaching safe use of blogging, forums and social networking sites(See Appendix 4 – draft letter to parents).

Videoconferencing
Videoconferencing uses the educational broadband network to ensure quality of service and security rather than the Internet. Pupils work with a supervising teacher when making or answering a videoconference call.

Managing emerging technologies
Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed. Children are not permitted to bring mobile phones in to the building; any phones brought to school should be handed into Reception for safe storage throughout the day. Visitors and staff should have mobiles phones switched off and put away safely when onsite during school hours. The sending of abusive or inappropriate text messages is forbidden. (see Anti-Bullying Policy)

Protecting Personal Data
Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Authorising Internet access
All staff and pupils must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource. The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date. Office staff will notify the ICT Assistant if a member of staff or pupil may leave and their access is immediately withdrawn by the ICT Support assistant or Subject leader. New users will be created and set up in the same way.

This policy should be read in conjunction with:
PDP Safeguarding Policy
PDP Social Networking Policy
PDP Whistleblowing Policy
PDP Anti bullying Policy
Acceptable Use of ICT Policy (PDJ and PDI)
PDP Policy for Information Communication Technology

Date Agreed: April 2014 **Review Date:** April 2016

Chair of Governors .....

Appendix 1:
Risk Assessment Log (to be completed annually)

Completed By: ICT Subject Leader **Date:**

Number	Activity	Risk	Likelihood	Impact	Score	Owner
1	Internet browsing	Access to inapropriate content				
2	Blogging	Inappropriate comments				
3	Staff laptops	Inappropriate use at home				
4						
5						
6						
7						

Likelihood: How likely is it that the risk could happen?
Impact: What would the impact be on the school?

Score for likelihood and Impact are between 1-3 (1 being the lowest)
Multiply likelihood and impact to achieve a score.

Score:
1-3 = Low Risk
4-6 = Medium Risk
7-9 = High Risk

Owner: The person who will action the risk assessment and make recommendations to the Head of School/Governing body.

Completed version to be stored in ICT Subject Folder and shared electronically with Senior Staff.

Risk Assessment

Risk Number	Risk
1	Children may be able to access inapropriate content through the school internet.
Likelihood	
Impact	
Risk Assesment	
Owner	ICT Subect Leader ICT Staff Class Teacher
Mitigation	

Approved / Not Approved Date:

Signed (Executive Headteacher): Signed (Governor):

Appendix 2:
E-Safety Incident Log

Reported by: (name of staff member)	Date:
Incident Description: (Describe what happened, involving which children and/or staff)	
Action taken:	
Signature:	Date:

Appendix 3:
Guidelines for Teaching E-safety

The following skills should be taught in the year groups listed, both when using the e-learning facilities in ICT lessons as well as in other subjects. Teachers should be aware that opportunities for reinforcing these guidelines may occur in many different circumstances and should always be utilised to make these rules second nature for the children.

Year Group	Skills / Knowledge
FS	Not to give their name, address or phone number to anyone; link to stranger danger talks. Online activities: http://www.kidsmart.org.uk/teachers/KS1/readsmartie.aspx *(Pupils will hear the story of Smartie the Penguin and answer associated questions throughout the story to help Smartie make the best decisions whilst on the internet. Pupils will learn a simple safety message in the form of a song, which will be repeated on several occasions.)*
1	Being kind to people, be polite in talking to them or writing to or about them. Know that what they do on the computer can be seen. Online activities: http://www.kidsmart.org.uk/teachers/ks1/digiduck.aspxDigiduck's *(Big Decision is a story for 3 to 7 year olds. It tells the story of Digiduck and his friends, and helps children understand how to be a good friend to others on the internet)*
2	Take responsibility for their own login details. Understand that they can be held responsible for things on their account. Internet – to only use sites approved by the teacher. Online activities: www.thinkuknow.co.uk/5_7/
3	Email and Text Messaging – politeness and safety. Reinforce that they must not give out their details to anyone, that people online may not be who they seem to be. Understand the need for netiquette; being polite online. Understand that Bullying online or through text messaging is unacceptable (Link to SEAL) Understand that they are responsible for what they look at on the internet, and that they must only look at appropriate materials. Introduce the mechanism of how to report if they find inappropriate materials; AUP and VLE whistle blowing tool Online activities: www.thinkuknow.co.uk/5_7/
4	Searching for appropriate terms and understand that not all material online is reliable, relevant or suitable. Understand the need to report instances of misuse or occurrences of inappropriate material. Recognise their own responsibility for their use of the Internet and that their online activities can be tracked. Online activities: www.childnet.com/kia/primary/smartadventure

5	As year 3 and 4, plus continue to reinforce the need for correct behaviour on the internet, and continual reinforcement of rules for researching using search engines and not giving out personal details. Introduce outside safety rules; not agreeing to meet anyone that they have spoken to online. Reinforce that people can pretend to be other than they are online, and they should assume that they are being lied to. Online activities: www.thinkuknow.co.uk/8_10/
6	As year 5, continue to reinforce safety guidelines.

All children will have access to the E-safety community on the VLE where they can access online resources and materials to support their understanding of these issues. Further materials and resources may be accessed via:
www.bbc.co.uk/cbbc/topics/stay-safe (site has a range of really good CBBC videos and resources to share with KS2 children)
www.childline.org.uk/Explore/OnlineSafety/Pages/OnlineSafety.aspx
www.kidsmart.org.uk/
www.kidscape.org.uk/childrenteens/cyberbullying.shtml
www.chatdanger.com/
hwww.childnet-int.org/
www.digitalme.co.uk/safe/
http://www.netsafe.org.nz/
http://www.saferinternet.org.uk/

It is the responsibility of all staff to equip our children with the skills they need to keep themselves safe in online environments. Don't assume that they will pick these skills up along the way – TEACH THEM!

Appendix 4: Draft annual letter to parents with Acceptable Use Policy

(To be sent out each September to all children)

E-safety at Parsons Down Partnership

Dear Parents and Carers,

Over the autumn term we will teach children how to use online environments safely and the importance of e-safety. It is essential that your children understand how to be safe online, communicate safely online using blogs and emails as well as how to use our shared network properly within school.

I have attached our Acceptable Use Policy for Junior School children and E-safety rules for Infant School children; please share these rules together with your child as they apply to using the Learning Platform and the school network. This document is very important and must be signed and returned to school as soon as possible. Children will not be able to use the ICT facilities provided at school until this form has been received. Any children who are not following these rules appropriately and within the terms of the school ICT agreement may have their access revoked.

In order to support and enhance your child's learning experience they will have access to our DB Primary Learning Platform. Your child can easily access the Learning Platform at home via our website: www.pdp.w-berks.sch.uk, by selecting Junior or Infant Learning Platform under the Pupil dropdown menu. The VLE is a secure site that only PDP children and staff can access. Children will be able to find a range of exciting year group and topic based communities which can be accessed inside and outside of school hours to develop their reading, writing and maths skills, as well as links to exciting games and activities. Homework can be submitted to teachers and uploaded into community areas rather than bringing memory sticks into school. Each child will be given their own personal username and password and we will encourage them not to share it with anyone else but their parents.

Children will be taught how to `whistle blow` which sends an email to their class teacher and to myself if they find any content of the VLE upsetting. However, if you or your child is at all concerned by anything on the VLE please do not hesitate to contact the school.

Our website this year also contains a calendar which will show important dates, reminders and newsletters which will be uploaded for you to access. Examples of excellent work from different classes and children will also be published for your child to share with you at home.

We hope you enjoy sharing this exciting online tool with your children at home!

Policy for the Acceptable Use of the School Network and Internet by Pupils
January 2013

Parsons Down Junior School promises to:

- Let you use the School's computers for learning.
- Keep you safe when using the Internet at School.
- Make sure any information about you is kept safe.
- Give clear rules for using the School's computers.

As a Pupil of Parsons Down Junior School you promise to:

☺ Get permission from a staff member before you use the School's computers.

☺ Be supervised by a member of staff when using the School network or internet.

☺ Keep all your password and log-in details secret – if someone finds out, tell your Teacher as soon as you can.

☺ Not give out your personal details, address or telephone number, or anyone else's, over the internet. Do not include this information on your DB homepage.

☺ Only access sites you have permission to use.

☺ Not download, use or upload any material, without permission from a member of staff.

☺ Not look at, upload onto the Learning Platform, or download any material, which may be unsuitable. If you are unsure about this or accidentally come across unsuitable material, you **must** tell a teacher.

☺ Not copy other people's work.

☺ Respect the privacy of files of other users. Only open and use the files that belong to you.

☺ Be polite and respect other people's views. The use of bad or inappropriate language or rude or aggressive behaviour is not allowed. This applies generally, but also in stored work, videos, e-mails, blogs, comments on the Learning Platform and on the school website.

☺ Allow your teacher, Head of School, Executive Headteacher or the ICT Staff to look at any material you store on the school network and the Learning Platform, this includes access your e-mails and uploaded documents.

☺ Not use portable storage devices, i.e. memory sticks, at school. Work can be emailed or uploaded onto the Learning Platform and accessed at school.

☺ Log off or shut down the computer when you have finished using it.

☺ Tell a member of staff if you see anyone breaking these rules. If you see any content on the Learning Platform which you are upset by tell staff by using the whistle blower tool.

☺ Tell a member of staff and use the whistle blower tool if you receive an unpleasant e-mail message. **DO NOT** delete it – your teacher of member of ICT staff will investigate it and delete it for you once they have dealt with the matter.

There is a copy of this policy on the School Website. Information on our School website is accessed using your email login and password.

There are consequences if you do not follow these rules. The Headteacher will be informed and a record will be kept of what has happened, and possibly one or more of the following:

☹ You may be banned from using the school network, internet, or accessing the Learning Platform and your email account.

☹ A letter will be sent telling your parents how you have broken the rules.

☹ The Headteacher of Parsons Down Junior School may give you a different punishment that they feel is appropriate.

This policy will be monitored by the ICT Coordinator and fully reviewed by the Full Governing Body annually.

Policy for the Acceptable Use of ICT, the School Network and Internet

I am signing to say that:

I understand and agree to follow the rules.
I understand what could happen if I break the rules.
I will tell a member of staff if I see anyone breaking these rules.

Child's Name (Please print) _____

Class _____

Signed _____

Parent/Carer Name (Please print) _____

Signed _____

Date _____

(Please sign and return to school)

E-Safety Rules

Think then Click

These rules help us to stay safe on the Internet

We only use and search the internet when an adult is with us

We can click on the buttons or links only when we know what they do.

We always ask an adult if we get lost on the Internet.

We open emails together with an adult.

We can write polite and friendly emails to people that we know.

Pupil's agreement

I understand the rules for using the computer.

I will always ask an adult for help using the computer so that I use it sensibly.

I know that adults will be able to see when I use the school's computers.

Signed / Marked…… Class ……

Child's Name……

Parent's Consent for Internet Access

I have read and understood the school e-safety rules and give permission for my son / daughter to access the internet. I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials but I appreciate that this is a difficult task.

I understand that the school cannot be held responsible for the content of materials accessed through the internet. I agree that the school is not liable for any damages arising from use of the internet facilities.

Please tick the box if you wish to have your child's username and password sent home. ☐

Signed ..... Date .....

Parsons Down Partnership of Schools
E-Safety Policy
April 2014

E-safety is a crucial area in protecting the wellbeing of the children across our Partnership as children are becoming more computer literate at younger ages. Technology offers unimaginable opportunities for education, communication and entertainment. Computers, mobile devices and gaming systems are constantly developing how and where children can access different online environments.

We aim to:

★ Develop informed learners who can identify and minimise risks, which may be amplified by technology.
★ Make children aware of their rights and responsibilities when working online so that they understand what makes safe and responsible online behaviour.
★ Educate children so they are clear and confident about how to report their concerns. As a Partnership, to have the appropriate mechanisms to intervene and support any incidents where appropriate.

Responsibility

E-safety provision is therefore a responsibility shared by staff, governors, parents and the pupils themselves.

- Parents: Supervising children during out of school hours; ensuring they are accessing suitable and age appropriate material; monitor use of social networking sites.
- Pupils: Responsible for the choices and decisions they make online when accessing content and communicating with others; adhere to the Acceptable Use Policy; follow the e-safety guidelines they have been taught and report any concerns.
- Staff: Supervise and monitor access whilst children are on site; teach children about responsible use and behaviour in an online environment; report and manage any e-safety incidents.
- ICT subject leader: Manage onsite filtering; monitor the coverage of teaching; provision and maintenance of equipment with support from the ICT Support Assistance.
- Senior Staff: Deal with any incidents of staff or children misuse and issue appropriate sanctions.
- Governors: Ensure a safe environment is provided for the children and monitor any issues which arise and ensure they are effectively dealt with.

Teaching and learning

The Internet is an essential element in 21st century life for education, business and social interaction. The Partnership has a duty to provide children with quality Internet access as part of their learning experience. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation. (See Appendix 3 - Guidelines for teaching E-Safety)

Risk Assessment

The Partnership will take all reasonable precautions to ensure that users access only appropriate material. Our Partnership operates a 'managed' system which provides opportunities for children to learn how to assess and manage risks in a safe environment. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. (See Appendix 1 – Risk Assessment Log) This log will be completed and monitored by the subject leader on an annual basis.

There are three main areas of risk which this policy focuses on covering:

1. Content: being exposed to illegal, inappropriate or harmful material.
2. Contact: being subjected to harmful online interaction with other users.
3. Conduct: personal online behaviour that increases the likelihood of, or causes harm.

Handling e-safety complaints

Complaints of Internet misuse will be dealt with by a senior member of staff. All issues will be logged on an incident sheet and monitored by the ICT subject leader (See Appendix 2 – E-safety Incident Log). Children who do not follow the agreed Acceptable Use Policy will receive appropriate sanctions depending on the incident. Access to the school network or VLE may be removed; instant red cards may be issued for incidents of racism, direct swearing or aggressive behaviour. Any complaint about staff misuse must be referred to the Head of School. Complaints of a child protection/safeguarding nature must be dealt with in accordance with the Partnership Child Protection/Safeguarding procedures (through the Executive Headteacher as designated Child Protection Officer).

Filtering

The Partnership Internet access is designed expressly for pupil use and includes filtering appropriate to the age of pupils. Pupils will be taught what Internet use is acceptable and what is not and give clear objectives for Internet use. Our Partnership operates a 'managed' system which provides opportunities for children to learn how to assess and manage risks in a safe environment. Filtering is monitored and managed within school following LA guidance to ensure systems to protect pupils are reviewed and improved. If staff or pupils discover an unsuitable site, it must be reported to the ICT subject leader. Pupils access is limited by filtering services

however staff have the ability to log in and access a wider range of sites, such as Youtube. Staff must not log children into blocked sites and must ensure they log off fully when leaving a machine.

Managing Network and Internet Access
Partnership ICT systems capacity and security will be reviewed regularly. All staff and pupils will be issued with user log-ons and passwords with differentiated rights and privileges. Sophos antivirus protection is updated regularly on all Partnership machines and laptops.
All pupils and staff with have access to their own personal storage space on the network, as well as access to specific shared drives, which they will be taught to use appropriately.

E-mail
Pupils are able to access their own personal email account through DB Primary. This is a closed email account which only allows them to send and receive emails from other school users. Pupils must immediately tell a teacher if they receive offensive e-mail in person or through the 'whistle blowing tool' on the VLE. Pupils must not reveal personal details of themselves or others in e-mail communication. Staff are issued with a secure Openhive Email Account which they can use in accordance with our Acceptable Use of ICT Policy. This email is also monitored by a filtering policy which may block some emails if their content is considered inappropriate. When appropriate it is possible for the ICT Subject Leader to request CAPITA to release and resend blocked emails to the recipient.

School web site
Our Partnership web site includes the school address, e-mail and telephone number. Staff or pupils' personal information will not be published. The Executive Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate. Photographs of children's work must not show pupils. Pupil's work and images can only be published with the permission of the pupil and parents. Pupils' full names will not be used anywhere on the Web site.

Social networking (please read in conjunction with Social Networking Policy)
The school will block access to social networking sites. Pupils and parents are advised that the use of social network spaces outside school is inappropriate for primary aged pupils. Pupils are able to access a monitored social networking site through the school's Virtual Learning Environment, DB Primary. This is tightly controlled and monitored by staff and is used for the purposes of teaching safe use of blogging, forums and social networking sites(See Appendix 4 – draft letter to parents).

Videoconferencing
Videoconferencing uses the educational broadband network to ensure quality of service and security rather than the Internet. Pupils work with a supervising teacher when making or answering a videoconference call.

Managing emerging technologies
Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed. Children are not permitted to bring mobile phones in to the building; any phones brought to school should be handed into Reception for safe storage throughout the day. Visitors and staff should have mobiles phones switched off and put away safely when onsite during school hours. The sending of abusive or inappropriate text messages is forbidden. (see Anti-Bullying Policy)

Protecting Personal Data
Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Authorising Internet access
All staff and pupils must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource. The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date. Office staff will notify the ICT Assistant if a member of staff or pupil may leave and their access is immediately withdrawn by the ICT Support assistant or Subject leader. New users will be created and set up in the same way.

This policy should be read in conjunction with:
PDP Safeguarding Policy
PDP Social Networking Policy
PDP Whistleblowing Policy
PDP Anti bullying Policy
Acceptable Use of ICT Policy (PDJ and PDI)
PDP Policy for Information Communication Technology

Date Agreed: April 2014 **Review Date:** April 2016

Chair of Governors .....

Appendix 1:
Risk Assessment Log (to be completed annually)

Completed By: ICT Subject Leader **Date:**

Number	Activity	Risk	Likelihood	Impact	Score	Owner
1	Internet browsing	Access to inapropriate content				
2	Blogging	Inappropriate comments				
3	Staff laptops	Inappropriate use at home				
4						
5						
6						
7						

Likelihood: How likely is it that the risk could happen?
Impact: What would the impact be on the school?

Score for likelihood and Impact are between 1-3 (1 being the lowest)
Multiply likelihood and impact to achieve a score.

Score:
1-3 = Low Risk
4-6 = Medium Risk
7-9 = High Risk

Owner: The person who will action the risk assessment and make recommendations to the Head of School/Governing body.

Completed version to be stored in ICT Subject Folder and shared electronically with Senior Staff.

Risk Assessment

Risk Number	Risk
1	Children may be able to access inapropriate content through the school internet.
Likelihood	
Impact	
Risk Assesment	
Owner	ICT Subect Leader ICT Staff Class Teacher
Mitigation	

Approved / Not Approved Date:

Signed (Executive Headteacher): Signed (Governor):

Appendix 2:
E-Safety Incident Log

Reported by: (name of staff member)	Date:
Incident Description: (Describe what happened, involving which children and/or staff)	
Action taken:	
Signature:	Date:

Appendix 3:
Guidelines for Teaching E-safety

The following skills should be taught in the year groups listed, both when using the e-learning facilities in ICT lessons as well as in other subjects. Teachers should be aware that opportunities for reinforcing these guidelines may occur in many different circumstances and should always be utilised to make these rules second nature for the children.

Year Group	Skills / Knowledge
FS	Not to give their name, address or phone number to anyone; link to stranger danger talks. Online activities: http://www.kidsmart.org.uk/teachers/KS1/readsmartie.aspx *(Pupils will hear the story of Smartie the Penguin and answer associated questions throughout the story to help Smartie make the best decisions whilst on the internet. Pupils will learn a simple safety message in the form of a song, which will be repeated on several occasions.)*
1	Being kind to people, be polite in talking to them or writing to or about them. Know that what they do on the computer can be seen. Online activities: http://www.kidsmart.org.uk/teachers/ks1/digiduck.aspxDigiduck's *(Big Decision is a story for 3 to 7 year olds. It tells the story of Digiduck and his friends, and helps children understand how to be a good friend to others on the internet)*
2	Take responsibility for their own login details. Understand that they can be held responsible for things on their account. Internet – to only use sites approved by the teacher. Online activities: www.thinkuknow.co.uk/5_7/
3	Email and Text Messaging – politeness and safety. Reinforce that they must not give out their details to anyone, that people online may not be who they seem to be. Understand the need for netiquette; being polite online. Understand that Bullying online or through text messaging is unacceptable (Link to SEAL) Understand that they are responsible for what they look at on the internet, and that they must only look at appropriate materials. Introduce the mechanism of how to report if they find inappropriate materials; AUP and VLE whistle blowing tool Online activities: www.thinkuknow.co.uk/5_7/
4	Searching for appropriate terms and understand that not all material online is reliable, relevant or suitable. Understand the need to report instances of misuse or occurrences of inappropriate material. Recognise their own responsibility for their use of the Internet and that their online activities can be tracked. Online activities: www.childnet.com/kia/primary/smartadventure

5	As year 3 and 4, plus continue to reinforce the need for correct behaviour on the internet, and continual reinforcement of rules for researching using search engines and not giving out personal details. Introduce outside safety rules; not agreeing to meet anyone that they have spoken to online. Reinforce that people can pretend to be other than they are online, and they should assume that they are being lied to. Online activities: www.thinkuknow.co.uk/8_10/
6	As year 5, continue to reinforce safety guidelines.

All children will have access to the E-safety community on the VLE where they can access online resources and materials to support their understanding of these issues. Further materials and resources may be accessed via:
www.bbc.co.uk/cbbc/topics/stay-safe (site has a range of really good CBBC videos and resources to share with KS2 children)
www.childline.org.uk/Explore/OnlineSafety/Pages/OnlineSafety.aspx
www.kidsmart.org.uk/
www.kidscape.org.uk/childrenteens/cyberbullying.shtml
www.chatdanger.com/
hwww.childnet-int.org/
www.digitalme.co.uk/safe/
http://www.netsafe.org.nz/
http://www.saferinternet.org.uk/

It is the responsibility of all staff to equip our children with the skills they need to keep themselves safe in online environments. Don't assume that they will pick these skills up along the way – TEACH THEM!

Appendix 4: Draft annual letter to parents with Acceptable Use Policy

(To be sent out each September to all children)

E-safety at Parsons Down Partnership

Dear Parents and Carers,

Over the autumn term we will teach children how to use online environments safely and the importance of e-safety. It is essential that your children understand how to be safe online, communicate safely online using blogs and emails as well as how to use our shared network properly within school.

I have attached our Acceptable Use Policy for Junior School children and E-safety rules for Infant School children; please share these rules together with your child as they apply to using the Learning Platform and the school network. This document is very important and must be signed and returned to school as soon as possible. Children will not be able to use the ICT facilities provided at school until this form has been received. Any children who are not following these rules appropriately and within the terms of the school ICT agreement may have their access revoked.

In order to support and enhance your child's learning experience they will have access to our DB Primary Learning Platform. Your child can easily access the Learning Platform at home via our website: www.pdp.w-berks.sch.uk, by selecting Junior or Infant Learning Platform under the Pupil dropdown menu. The VLE is a secure site that only PDP children and staff can access. Children will be able to find a range of exciting year group and topic based communities which can be accessed inside and outside of school hours to develop their reading, writing and maths skills, as well as links to exciting games and activities. Homework can be submitted to teachers and uploaded into community areas rather than bringing memory sticks into school. Each child will be given their own personal username and password and we will encourage them not to share it with anyone else but their parents.

Children will be taught how to `whistle blow` which sends an email to their class teacher and to myself if they find any content of the VLE upsetting. However, if you or your child is at all concerned by anything on the VLE please do not hesitate to contact the school.

Our website this year also contains a calendar which will show important dates, reminders and newsletters which will be uploaded for you to access. Examples of excellent work from different classes and children will also be published for your child to share with you at home.

We hope you enjoy sharing this exciting online tool with your children at home!

Policy for the Acceptable Use of the School Network and Internet by Pupils
January 2013

Parsons Down Junior School promises to:

- Let you use the School's computers for learning.
- Keep you safe when using the Internet at School.
- Make sure any information about you is kept safe.
- Give clear rules for using the School's computers.

As a Pupil of Parsons Down Junior School you promise to:

☺ Get permission from a staff member before you use the School's computers.

☺ Be supervised by a member of staff when using the School network or internet.

☺ Keep all your password and log-in details secret – if someone finds out, tell your Teacher as soon as you can.

☺ Not give out your personal details, address or telephone number, or anyone else's, over the internet. Do not include this information on your DB homepage.

☺ Only access sites you have permission to use.

☺ Not download, use or upload any material, without permission from a member of staff.

☺ Not look at, upload onto the Learning Platform, or download any material, which may be unsuitable. If you are unsure about this or accidentally come across unsuitable material, you **must** tell a teacher.

☺ Not copy other people's work.

☺ Respect the privacy of files of other users. Only open and use the files that belong to you.

☺ Be polite and respect other people's views. The use of bad or inappropriate language or rude or aggressive behaviour is not allowed. This applies generally, but also in stored work, videos, e-mails, blogs, comments on the Learning Platform and on the school website.

☺ Allow your teacher, Head of School, Executive Headteacher or the ICT Staff to look at any material you store on the school network and the Learning Platform, this includes access your e-mails and uploaded documents.

☺ Not use portable storage devices, i.e. memory sticks, at school. Work can be emailed or uploaded onto the Learning Platform and accessed at school.

☺ Log off or shut down the computer when you have finished using it.

☺ Tell a member of staff if you see anyone breaking these rules. If you see any content on the Learning Platform which you are upset by tell staff by using the whistle blower tool.

☺ Tell a member of staff and use the whistle blower tool if you receive an unpleasant e-mail message. **DO NOT** delete it – your teacher of member of ICT staff will investigate it and delete it for you once they have dealt with the matter.

There is a copy of this policy on the School Website. Information on our School website is accessed using your email login and password.

There are consequences if you do not follow these rules. The Headteacher will be informed and a record will be kept of what has happened, and possibly one or more of the following:

☹ You may be banned from using the school network, internet, or accessing the Learning Platform and your email account.

☹ A letter will be sent telling your parents how you have broken the rules.

☹ The Headteacher of Parsons Down Junior School may give you a different punishment that they feel is appropriate.

This policy will be monitored by the ICT Coordinator and fully reviewed by the Full Governing Body annually.

Policy for the Acceptable Use of ICT, the School Network and Internet

I am signing to say that:

I understand and agree to follow the rules.
I understand what could happen if I break the rules.
I will tell a member of staff if I see anyone breaking these rules.

Child's Name (Please print) _____

Class _____

Signed _____

Parent/Carer Name (Please print) _____

Signed _____

Date _____

(Please sign and return to school)

E-Safety Rules

Think then Click

These rules help us to stay safe on the Internet

We only use and search the internet when an adult is with us

We can click on the buttons or links only when we know what they do.

We always ask an adult if we get lost on the Internet.

We open emails together with an adult.

We can write polite and friendly emails to people that we know.

Pupil's agreement

I understand the rules for using the computer.

I will always ask an adult for help using the computer so that I use it sensibly.

I know that adults will be able to see when I use the school's computers.

Signed / Marked…… Class ……

Child's Name……

Parent's Consent for Internet Access

I have read and understood the school e-safety rules and give permission for my son / daughter to access the internet. I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials but I appreciate that this is a difficult task.

I understand that the school cannot be held responsible for the content of materials accessed through the internet. I agree that the school is not liable for any damages arising from use of the internet facilities.

Please tick the box if you wish to have your child's username and password sent home. ☐

Signed ..... Date .....

Parsons Down Partnership of Schools
E-Safety Policy
April 2014

E-safety is a crucial area in protecting the wellbeing of the children across our Partnership as children are becoming more computer literate at younger ages. Technology offers unimaginable opportunities for education, communication and entertainment. Computers, mobile devices and gaming systems are constantly developing how and where children can access different online environments.

We aim to:

★ Develop informed learners who can identify and minimise risks, which may be amplified by technology.
★ Make children aware of their rights and responsibilities when working online so that they understand what makes safe and responsible online behaviour.
★ Educate children so they are clear and confident about how to report their concerns. As a Partnership, to have the appropriate mechanisms to intervene and support any incidents where appropriate.

Responsibility

E-safety provision is therefore a responsibility shared by staff, governors, parents and the pupils themselves.

- Parents: Supervising children during out of school hours; ensuring they are accessing suitable and age appropriate material; monitor use of social networking sites.
- Pupils: Responsible for the choices and decisions they make online when accessing content and communicating with others; adhere to the Acceptable Use Policy; follow the e-safety guidelines they have been taught and report any concerns.
- Staff: Supervise and monitor access whilst children are on site; teach children about responsible use and behaviour in an online environment; report and manage any e-safety incidents.
- ICT subject leader: Manage onsite filtering; monitor the coverage of teaching; provision and maintenance of equipment with support from the ICT Support Assistance.
- Senior Staff: Deal with any incidents of staff or children misuse and issue appropriate sanctions.
- Governors: Ensure a safe environment is provided for the children and monitor any issues which arise and ensure they are effectively dealt with.

Teaching and learning

The Internet is an essential element in 21st century life for education, business and social interaction. The Partnership has a duty to provide children with quality Internet access as part of their learning experience. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation. (See Appendix 3 - Guidelines for teaching E-Safety)

Risk Assessment

The Partnership will take all reasonable precautions to ensure that users access only appropriate material. Our Partnership operates a 'managed' system which provides opportunities for children to learn how to assess and manage risks in a safe environment. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. (See Appendix 1 – Risk Assessment Log) This log will be completed and monitored by the subject leader on an annual basis.

There are three main areas of risk which this policy focuses on covering:

1. Content: being exposed to illegal, inappropriate or harmful material.
2. Contact: being subjected to harmful online interaction with other users.
3. Conduct: personal online behaviour that increases the likelihood of, or causes harm.

Handling e-safety complaints

Complaints of Internet misuse will be dealt with by a senior member of staff. All issues will be logged on an incident sheet and monitored by the ICT subject leader (See Appendix 2 – E-safety Incident Log). Children who do not follow the agreed Acceptable Use Policy will receive appropriate sanctions depending on the incident. Access to the school network or VLE may be removed; instant red cards may be issued for incidents of racism, direct swearing or aggressive behaviour. Any complaint about staff misuse must be referred to the Head of School. Complaints of a child protection/safeguarding nature must be dealt with in accordance with the Partnership Child Protection/Safeguarding procedures (through the Executive Headteacher as designated Child Protection Officer).

Filtering

The Partnership Internet access is designed expressly for pupil use and includes filtering appropriate to the age of pupils. Pupils will be taught what Internet use is acceptable and what is not and give clear objectives for Internet use. Our Partnership operates a 'managed' system which provides opportunities for children to learn how to assess and manage risks in a safe environment. Filtering is monitored and managed within school following LA guidance to ensure systems to protect pupils are reviewed and improved. If staff or pupils discover an unsuitable site, it must be reported to the ICT subject leader. Pupils access is limited by filtering services

however staff have the ability to log in and access a wider range of sites, such as Youtube. Staff must not log children into blocked sites and must ensure they log off fully when leaving a machine.

Managing Network and Internet Access
Partnership ICT systems capacity and security will be reviewed regularly. All staff and pupils will be issued with user log-ons and passwords with differentiated rights and privileges. Sophos antivirus protection is updated regularly on all Partnership machines and laptops.
All pupils and staff with have access to their own personal storage space on the network, as well as access to specific shared drives, which they will be taught to use appropriately.

E-mail
Pupils are able to access their own personal email account through DB Primary. This is a closed email account which only allows them to send and receive emails from other school users. Pupils must immediately tell a teacher if they receive offensive e-mail in person or through the 'whistle blowing tool' on the VLE. Pupils must not reveal personal details of themselves or others in e-mail communication. Staff are issued with a secure Openhive Email Account which they can use in accordance with our Acceptable Use of ICT Policy. This email is also monitored by a filtering policy which may block some emails if their content is considered inappropriate. When appropriate it is possible for the ICT Subject Leader to request CAPITA to release and resend blocked emails to the recipient.

School web site
Our Partnership web site includes the school address, e-mail and telephone number. Staff or pupils' personal information will not be published. The Executive Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate. Photographs of children's work must not show pupils. Pupil's work and images can only be published with the permission of the pupil and parents. Pupils' full names will not be used anywhere on the Web site.

Social networking (please read in conjunction with Social Networking Policy)
The school will block access to social networking sites. Pupils and parents are advised that the use of social network spaces outside school is inappropriate for primary aged pupils. Pupils are able to access a monitored social networking site through the school's Virtual Learning Environment, DB Primary. This is tightly controlled and monitored by staff and is used for the purposes of teaching safe use of blogging, forums and social networking sites(See Appendix 4 – draft letter to parents).

Videoconferencing
Videoconferencing uses the educational broadband network to ensure quality of service and security rather than the Internet. Pupils work with a supervising teacher when making or answering a videoconference call.

Managing emerging technologies
Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed. Children are not permitted to bring mobile phones in to the building; any phones brought to school should be handed into Reception for safe storage throughout the day. Visitors and staff should have mobiles phones switched off and put away safely when onsite during school hours. The sending of abusive or inappropriate text messages is forbidden. (see Anti-Bullying Policy)

Protecting Personal Data
Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Authorising Internet access
All staff and pupils must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource. The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date. Office staff will notify the ICT Assistant if a member of staff or pupil may leave and their access is immediately withdrawn by the ICT Support assistant or Subject leader. New users will be created and set up in the same way.

This policy should be read in conjunction with:
PDP Safeguarding Policy
PDP Social Networking Policy
PDP Whistleblowing Policy
PDP Anti bullying Policy
Acceptable Use of ICT Policy (PDJ and PDI)
PDP Policy for Information Communication Technology

Date Agreed: April 2014 **Review Date:** April 2016

Chair of Governors .....

Appendix 1:
Risk Assessment Log (to be completed annually)

Completed By: ICT Subject Leader **Date:**

Number	Activity	Risk	Likelihood	Impact	Score	Owner
1	Internet browsing	Access to inapropriate content				
2	Blogging	Inappropriate comments				
3	Staff laptops	Inappropriate use at home				
4						
5						
6						
7						

Likelihood: How likely is it that the risk could happen?
Impact: What would the impact be on the school?

Score for likelihood and Impact are between 1-3 (1 being the lowest)
Multiply likelihood and impact to achieve a score.

Score:
1-3 = Low Risk
4-6 = Medium Risk
7-9 = High Risk

Owner: The person who will action the risk assessment and make recommendations to the Head of School/Governing body.

Completed version to be stored in ICT Subject Folder and shared electronically with Senior Staff.

Risk Assessment

Risk Number	Risk
1	Children may be able to access inapropriate content through the school internet.
Likelihood	
Impact	
Risk Assesment	
Owner	ICT Subect Leader ICT Staff Class Teacher
Mitigation	

Approved / Not Approved Date:

Signed (Executive Headteacher): Signed (Governor):

Appendix 2:
E-Safety Incident Log

Reported by: (name of staff member)	Date:
Incident Description: (Describe what happened, involving which children and/or staff)	
Action taken:	
Signature:	Date:

Appendix 3:
Guidelines for Teaching E-safety

The following skills should be taught in the year groups listed, both when using the e-learning facilities in ICT lessons as well as in other subjects. Teachers should be aware that opportunities for reinforcing these guidelines may occur in many different circumstances and should always be utilised to make these rules second nature for the children.

Year Group	Skills / Knowledge
FS	Not to give their name, address or phone number to anyone; link to stranger danger talks. Online activities: http://www.kidsmart.org.uk/teachers/KS1/readsmartie.aspx *(Pupils will hear the story of Smartie the Penguin and answer associated questions throughout the story to help Smartie make the best decisions whilst on the internet. Pupils will learn a simple safety message in the form of a song, which will be repeated on several occasions.)*
1	Being kind to people, be polite in talking to them or writing to or about them. Know that what they do on the computer can be seen. Online activities: http://www.kidsmart.org.uk/teachers/ks1/digiduck.aspxDigiduck's *(Big Decision is a story for 3 to 7 year olds. It tells the story of Digiduck and his friends, and helps children understand how to be a good friend to others on the internet)*
2	Take responsibility for their own login details. Understand that they can be held responsible for things on their account. Internet – to only use sites approved by the teacher. Online activities: www.thinkuknow.co.uk/5_7/
3	Email and Text Messaging – politeness and safety. Reinforce that they must not give out their details to anyone, that people online may not be who they seem to be. Understand the need for netiquette; being polite online. Understand that Bullying online or through text messaging is unacceptable (Link to SEAL) Understand that they are responsible for what they look at on the internet, and that they must only look at appropriate materials. Introduce the mechanism of how to report if they find inappropriate materials; AUP and VLE whistle blowing tool Online activities: www.thinkuknow.co.uk/5_7/
4	Searching for appropriate terms and understand that not all material online is reliable, relevant or suitable. Understand the need to report instances of misuse or occurrences of inappropriate material. Recognise their own responsibility for their use of the Internet and that their online activities can be tracked. Online activities: www.childnet.com/kia/primary/smartadventure

5	As year 3 and 4, plus continue to reinforce the need for correct behaviour on the internet, and continual reinforcement of rules for researching using search engines and not giving out personal details. Introduce outside safety rules; not agreeing to meet anyone that they have spoken to online. Reinforce that people can pretend to be other than they are online, and they should assume that they are being lied to. Online activities: www.thinkuknow.co.uk/8_10/
6	As year 5, continue to reinforce safety guidelines.

All children will have access to the E-safety community on the VLE where they can access online resources and materials to support their understanding of these issues. Further materials and resources may be accessed via:
www.bbc.co.uk/cbbc/topics/stay-safe (site has a range of really good CBBC videos and resources to share with KS2 children)
www.childline.org.uk/Explore/OnlineSafety/Pages/OnlineSafety.aspx
www.kidsmart.org.uk/
www.kidscape.org.uk/childrenteens/cyberbullying.shtml
www.chatdanger.com/
hwww.childnet-int.org/
www.digitalme.co.uk/safe/
http://www.netsafe.org.nz/
http://www.saferinternet.org.uk/

It is the responsibility of all staff to equip our children with the skills they need to keep themselves safe in online environments. Don't assume that they will pick these skills up along the way – TEACH THEM!

Appendix 4: Draft annual letter to parents with Acceptable Use Policy

(To be sent out each September to all children)

E-safety at Parsons Down Partnership

Dear Parents and Carers,

Over the autumn term we will teach children how to use online environments safely and the importance of e-safety. It is essential that your children understand how to be safe online, communicate safely online using blogs and emails as well as how to use our shared network properly within school.

I have attached our Acceptable Use Policy for Junior School children and E-safety rules for Infant School children; please share these rules together with your child as they apply to using the Learning Platform and the school network. This document is very important and must be signed and returned to school as soon as possible. Children will not be able to use the ICT facilities provided at school until this form has been received. Any children who are not following these rules appropriately and within the terms of the school ICT agreement may have their access revoked.

In order to support and enhance your child's learning experience they will have access to our DB Primary Learning Platform. Your child can easily access the Learning Platform at home via our website: www.pdp.w-berks.sch.uk, by selecting Junior or Infant Learning Platform under the Pupil dropdown menu. The VLE is a secure site that only PDP children and staff can access. Children will be able to find a range of exciting year group and topic based communities which can be accessed inside and outside of school hours to develop their reading, writing and maths skills, as well as links to exciting games and activities. Homework can be submitted to teachers and uploaded into community areas rather than bringing memory sticks into school. Each child will be given their own personal username and password and we will encourage them not to share it with anyone else but their parents.

Children will be taught how to `whistle blow` which sends an email to their class teacher and to myself if they find any content of the VLE upsetting. However, if you or your child is at all concerned by anything on the VLE please do not hesitate to contact the school.

Our website this year also contains a calendar which will show important dates, reminders and newsletters which will be uploaded for you to access. Examples of excellent work from different classes and children will also be published for your child to share with you at home.

We hope you enjoy sharing this exciting online tool with your children at home!

Policy for the Acceptable Use of the School Network and Internet by Pupils
January 2013

Parsons Down Junior School promises to:

- Let you use the School's computers for learning.
- Keep you safe when using the Internet at School.
- Make sure any information about you is kept safe.
- Give clear rules for using the School's computers.

As a Pupil of Parsons Down Junior School you promise to:

☺ Get permission from a staff member before you use the School's computers.

☺ Be supervised by a member of staff when using the School network or internet.

☺ Keep all your password and log-in details secret – if someone finds out, tell your Teacher as soon as you can.

☺ Not give out your personal details, address or telephone number, or anyone else's, over the internet. Do not include this information on your DB homepage.

☺ Only access sites you have permission to use.

☺ Not download, use or upload any material, without permission from a member of staff.

☺ Not look at, upload onto the Learning Platform, or download any material, which may be unsuitable. If you are unsure about this or accidentally come across unsuitable material, you **must** tell a teacher.

☺ Not copy other people's work.

☺ Respect the privacy of files of other users. Only open and use the files that belong to you.

☺ Be polite and respect other people's views. The use of bad or inappropriate language or rude or aggressive behaviour is not allowed. This applies generally, but also in stored work, videos, e-mails, blogs, comments on the Learning Platform and on the school website.

☺ Allow your teacher, Head of School, Executive Headteacher or the ICT Staff to look at any material you store on the school network and the Learning Platform, this includes access your e-mails and uploaded documents.

☺ Not use portable storage devices, i.e. memory sticks, at school. Work can be emailed or uploaded onto the Learning Platform and accessed at school.

☺ Log off or shut down the computer when you have finished using it.

☺ Tell a member of staff if you see anyone breaking these rules. If you see any content on the Learning Platform which you are upset by tell staff by using the whistle blower tool.

☺ Tell a member of staff and use the whistle blower tool if you receive an unpleasant e-mail message. **DO NOT** delete it – your teacher of member of ICT staff will investigate it and delete it for you once they have dealt with the matter.

There is a copy of this policy on the School Website. Information on our School website is accessed using your email login and password.

There are consequences if you do not follow these rules. The Headteacher will be informed and a record will be kept of what has happened, and possibly one or more of the following:

☹ You may be banned from using the school network, internet, or accessing the Learning Platform and your email account.

☹ A letter will be sent telling your parents how you have broken the rules.

☹ The Headteacher of Parsons Down Junior School may give you a different punishment that they feel is appropriate.

This policy will be monitored by the ICT Coordinator and fully reviewed by the Full Governing Body annually.

Policy for the Acceptable Use of ICT, the School Network and Internet

I am signing to say that:

I understand and agree to follow the rules.
I understand what could happen if I break the rules.
I will tell a member of staff if I see anyone breaking these rules.

Child's Name (Please print) _____

Class _____

Signed _____

Parent/Carer Name (Please print) _____

Signed _____

Date _____

(Please sign and return to school)

E-Safety Rules

Think then Click

These rules help us to stay safe on the Internet

We only use and search the internet when an adult is with us

We can click on the buttons or links only when we know what they do.

We always ask an adult if we get lost on the Internet.

We open emails together with an adult.

We can write polite and friendly emails to people that we know.

Pupil's agreement

I understand the rules for using the computer.

I will always ask an adult for help using the computer so that I use it sensibly.

I know that adults will be able to see when I use the school's computers.

Signed / Marked…… Class ……

Child's Name……

Parent's Consent for Internet Access

I have read and understood the school e-safety rules and give permission for my son / daughter to access the internet. I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials but I appreciate that this is a difficult task.

I understand that the school cannot be held responsible for the content of materials accessed through the internet. I agree that the school is not liable for any damages arising from use of the internet facilities.

Please tick the box if you wish to have your child's username and password sent home. ☐

Signed ..... Date .....

Parsons Down Partnership of Schools
E-Safety Policy
April 2014

E-safety is a crucial area in protecting the wellbeing of the children across our Partnership as children are becoming more computer literate at younger ages. Technology offers unimaginable opportunities for education, communication and entertainment. Computers, mobile devices and gaming systems are constantly developing how and where children can access different online environments.

We aim to:

★ Develop informed learners who can identify and minimise risks, which may be amplified by technology.
★ Make children aware of their rights and responsibilities when working online so that they understand what makes safe and responsible online behaviour.
★ Educate children so they are clear and confident about how to report their concerns. As a Partnership, to have the appropriate mechanisms to intervene and support any incidents where appropriate.

Responsibility

E-safety provision is therefore a responsibility shared by staff, governors, parents and the pupils themselves.

- Parents: Supervising children during out of school hours; ensuring they are accessing suitable and age appropriate material; monitor use of social networking sites.
- Pupils: Responsible for the choices and decisions they make online when accessing content and communicating with others; adhere to the Acceptable Use Policy; follow the e-safety guidelines they have been taught and report any concerns.
- Staff: Supervise and monitor access whilst children are on site; teach children about responsible use and behaviour in an online environment; report and manage any e-safety incidents.
- ICT subject leader: Manage onsite filtering; monitor the coverage of teaching; provision and maintenance of equipment with support from the ICT Support Assistance.
- Senior Staff: Deal with any incidents of staff or children misuse and issue appropriate sanctions.
- Governors: Ensure a safe environment is provided for the children and monitor any issues which arise and ensure they are effectively dealt with.

Teaching and learning

The Internet is an essential element in 21st century life for education, business and social interaction. The Partnership has a duty to provide children with quality Internet access as part of their learning experience. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation. (See Appendix 3 - Guidelines for teaching E-Safety)

Risk Assessment

The Partnership will take all reasonable precautions to ensure that users access only appropriate material. Our Partnership operates a 'managed' system which provides opportunities for children to learn how to assess and manage risks in a safe environment. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. (See Appendix 1 – Risk Assessment Log) This log will be completed and monitored by the subject leader on an annual basis.

There are three main areas of risk which this policy focuses on covering:

1. Content: being exposed to illegal, inappropriate or harmful material.
2. Contact: being subjected to harmful online interaction with other users.
3. Conduct: personal online behaviour that increases the likelihood of, or causes harm.

Handling e-safety complaints

Complaints of Internet misuse will be dealt with by a senior member of staff. All issues will be logged on an incident sheet and monitored by the ICT subject leader (See Appendix 2 – E-safety Incident Log). Children who do not follow the agreed Acceptable Use Policy will receive appropriate sanctions depending on the incident. Access to the school network or VLE may be removed; instant red cards may be issued for incidents of racism, direct swearing or aggressive behaviour. Any complaint about staff misuse must be referred to the Head of School. Complaints of a child protection/safeguarding nature must be dealt with in accordance with the Partnership Child Protection/Safeguarding procedures (through the Executive Headteacher as designated Child Protection Officer).

Filtering

The Partnership Internet access is designed expressly for pupil use and includes filtering appropriate to the age of pupils. Pupils will be taught what Internet use is acceptable and what is not and give clear objectives for Internet use. Our Partnership operates a 'managed' system which provides opportunities for children to learn how to assess and manage risks in a safe environment. Filtering is monitored and managed within school following LA guidance to ensure systems to protect pupils are reviewed and improved. If staff or pupils discover an unsuitable site, it must be reported to the ICT subject leader. Pupils access is limited by filtering services

however staff have the ability to log in and access a wider range of sites, such as Youtube. Staff must not log children into blocked sites and must ensure they log off fully when leaving a machine.

Managing Network and Internet Access
Partnership ICT systems capacity and security will be reviewed regularly. All staff and pupils will be issued with user log-ons and passwords with differentiated rights and privileges. Sophos antivirus protection is updated regularly on all Partnership machines and laptops.
All pupils and staff with have access to their own personal storage space on the network, as well as access to specific shared drives, which they will be taught to use appropriately.

E-mail
Pupils are able to access their own personal email account through DB Primary. This is a closed email account which only allows them to send and receive emails from other school users. Pupils must immediately tell a teacher if they receive offensive e-mail in person or through the 'whistle blowing tool' on the VLE. Pupils must not reveal personal details of themselves or others in e-mail communication. Staff are issued with a secure Openhive Email Account which they can use in accordance with our Acceptable Use of ICT Policy. This email is also monitored by a filtering policy which may block some emails if their content is considered inappropriate. When appropriate it is possible for the ICT Subject Leader to request CAPITA to release and resend blocked emails to the recipient.

School web site
Our Partnership web site includes the school address, e-mail and telephone number. Staff or pupils' personal information will not be published. The Executive Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate. Photographs of children's work must not show pupils. Pupil's work and images can only be published with the permission of the pupil and parents. Pupils' full names will not be used anywhere on the Web site.

Social networking (please read in conjunction with Social Networking Policy)
The school will block access to social networking sites. Pupils and parents are advised that the use of social network spaces outside school is inappropriate for primary aged pupils. Pupils are able to access a monitored social networking site through the school's Virtual Learning Environment, DB Primary. This is tightly controlled and monitored by staff and is used for the purposes of teaching safe use of blogging, forums and social networking sites(See Appendix 4 – draft letter to parents).

Videoconferencing
Videoconferencing uses the educational broadband network to ensure quality of service and security rather than the Internet. Pupils work with a supervising teacher when making or answering a videoconference call.

Managing emerging technologies
Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed. Children are not permitted to bring mobile phones in to the building; any phones brought to school should be handed into Reception for safe storage throughout the day. Visitors and staff should have mobiles phones switched off and put away safely when onsite during school hours. The sending of abusive or inappropriate text messages is forbidden. (see Anti-Bullying Policy)

Protecting Personal Data
Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Authorising Internet access
All staff and pupils must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource. The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date. Office staff will notify the ICT Assistant if a member of staff or pupil may leave and their access is immediately withdrawn by the ICT Support assistant or Subject leader. New users will be created and set up in the same way.

This policy should be read in conjunction with:
PDP Safeguarding Policy
PDP Social Networking Policy
PDP Whistleblowing Policy
PDP Anti bullying Policy
Acceptable Use of ICT Policy (PDJ and PDI)
PDP Policy for Information Communication Technology

Date Agreed: April 2014 **Review Date:** April 2016

Chair of Governors .....

Appendix 1:
Risk Assessment Log (to be completed annually)

Completed By: ICT Subject Leader **Date:**

Number	Activity	Risk	Likelihood	Impact	Score	Owner
1	Internet browsing	Access to inapropriate content				
2	Blogging	Inappropriate comments				
3	Staff laptops	Inappropriate use at home				
4						
5						
6						
7						

Likelihood: How likely is it that the risk could happen?
Impact: What would the impact be on the school?

Score for likelihood and Impact are between 1-3 (1 being the lowest)
Multiply likelihood and impact to achieve a score.

Score:
1-3 = Low Risk
4-6 = Medium Risk
7-9 = High Risk

Owner: The person who will action the risk assessment and make recommendations to the Head of School/Governing body.

Completed version to be stored in ICT Subject Folder and shared electronically with Senior Staff.

Risk Assessment

Risk Number	Risk
1	Children may be able to access inapropriate content through the school internet.
Likelihood	
Impact	
Risk Assesment	
Owner	ICT Subect Leader ICT Staff Class Teacher
Mitigation	

Approved / Not Approved Date:

Signed (Executive Headteacher): Signed (Governor):

Appendix 2:
E-Safety Incident Log

Reported by: (name of staff member)	Date:
Incident Description: (Describe what happened, involving which children and/or staff)	
Action taken:	
Signature:	Date:

Appendix 3:
Guidelines for Teaching E-safety

The following skills should be taught in the year groups listed, both when using the e-learning facilities in ICT lessons as well as in other subjects. Teachers should be aware that opportunities for reinforcing these guidelines may occur in many different circumstances and should always be utilised to make these rules second nature for the children.

Year Group	Skills / Knowledge
FS	Not to give their name, address or phone number to anyone; link to stranger danger talks. Online activities: http://www.kidsmart.org.uk/teachers/KS1/readsmartie.aspx *(Pupils will hear the story of Smartie the Penguin and answer associated questions throughout the story to help Smartie make the best decisions whilst on the internet. Pupils will learn a simple safety message in the form of a song, which will be repeated on several occasions.)*
1	Being kind to people, be polite in talking to them or writing to or about them. Know that what they do on the computer can be seen. Online activities: http://www.kidsmart.org.uk/teachers/ks1/digiduck.aspxDigiduck's *(Big Decision is a story for 3 to 7 year olds. It tells the story of Digiduck and his friends, and helps children understand how to be a good friend to others on the internet)*
2	Take responsibility for their own login details. Understand that they can be held responsible for things on their account. Internet – to only use sites approved by the teacher. Online activities: www.thinkuknow.co.uk/5_7/
3	Email and Text Messaging – politeness and safety. Reinforce that they must not give out their details to anyone, that people online may not be who they seem to be. Understand the need for netiquette; being polite online. Understand that Bullying online or through text messaging is unacceptable (Link to SEAL) Understand that they are responsible for what they look at on the internet, and that they must only look at appropriate materials. Introduce the mechanism of how to report if they find inappropriate materials; AUP and VLE whistle blowing tool Online activities: www.thinkuknow.co.uk/5_7/
4	Searching for appropriate terms and understand that not all material online is reliable, relevant or suitable. Understand the need to report instances of misuse or occurrences of inappropriate material. Recognise their own responsibility for their use of the Internet and that their online activities can be tracked. Online activities: www.childnet.com/kia/primary/smartadventure

5	As year 3 and 4, plus continue to reinforce the need for correct behaviour on the internet, and continual reinforcement of rules for researching using search engines and not giving out personal details. Introduce outside safety rules; not agreeing to meet anyone that they have spoken to online. Reinforce that people can pretend to be other than they are online, and they should assume that they are being lied to. Online activities: www.thinkuknow.co.uk/8_10/
6	As year 5, continue to reinforce safety guidelines.

All children will have access to the E-safety community on the VLE where they can access online resources and materials to support their understanding of these issues. Further materials and resources may be accessed via:
www.bbc.co.uk/cbbc/topics/stay-safe (site has a range of really good CBBC videos and resources to share with KS2 children)
www.childline.org.uk/Explore/OnlineSafety/Pages/OnlineSafety.aspx
www.kidsmart.org.uk/
www.kidscape.org.uk/childrenteens/cyberbullying.shtml
www.chatdanger.com/
hwww.childnet-int.org/
www.digitalme.co.uk/safe/
http://www.netsafe.org.nz/
http://www.saferinternet.org.uk/

It is the responsibility of all staff to equip our children with the skills they need to keep themselves safe in online environments. Don't assume that they will pick these skills up along the way – TEACH THEM!

Appendix 4: Draft annual letter to parents with Acceptable Use Policy

(To be sent out each September to all children)

E-safety at Parsons Down Partnership

Dear Parents and Carers,

Over the autumn term we will teach children how to use online environments safely and the importance of e-safety. It is essential that your children understand how to be safe online, communicate safely online using blogs and emails as well as how to use our shared network properly within school.

I have attached our Acceptable Use Policy for Junior School children and E-safety rules for Infant School children; please share these rules together with your child as they apply to using the Learning Platform and the school network. This document is very important and must be signed and returned to school as soon as possible. Children will not be able to use the ICT facilities provided at school until this form has been received. Any children who are not following these rules appropriately and within the terms of the school ICT agreement may have their access revoked.

In order to support and enhance your child's learning experience they will have access to our DB Primary Learning Platform. Your child can easily access the Learning Platform at home via our website: www.pdp.w-berks.sch.uk, by selecting Junior or Infant Learning Platform under the Pupil dropdown menu. The VLE is a secure site that only PDP children and staff can access. Children will be able to find a range of exciting year group and topic based communities which can be accessed inside and outside of school hours to develop their reading, writing and maths skills, as well as links to exciting games and activities. Homework can be submitted to teachers and uploaded into community areas rather than bringing memory sticks into school. Each child will be given their own personal username and password and we will encourage them not to share it with anyone else but their parents.

Children will be taught how to `whistle blow` which sends an email to their class teacher and to myself if they find any content of the VLE upsetting. However, if you or your child is at all concerned by anything on the VLE please do not hesitate to contact the school.

Our website this year also contains a calendar which will show important dates, reminders and newsletters which will be uploaded for you to access. Examples of excellent work from different classes and children will also be published for your child to share with you at home.

We hope you enjoy sharing this exciting online tool with your children at home!

Policy for the Acceptable Use of the School Network and Internet by Pupils
January 2013

Parsons Down Junior School promises to:

- Let you use the School's computers for learning.
- Keep you safe when using the Internet at School.
- Make sure any information about you is kept safe.
- Give clear rules for using the School's computers.

As a Pupil of Parsons Down Junior School you promise to:

☺ Get permission from a staff member before you use the School's computers.

☺ Be supervised by a member of staff when using the School network or internet.

☺ Keep all your password and log-in details secret – if someone finds out, tell your Teacher as soon as you can.

☺ Not give out your personal details, address or telephone number, or anyone else's, over the internet. Do not include this information on your DB homepage.

☺ Only access sites you have permission to use.

☺ Not download, use or upload any material, without permission from a member of staff.

☺ Not look at, upload onto the Learning Platform, or download any material, which may be unsuitable. If you are unsure about this or accidentally come across unsuitable material, you **must** tell a teacher.

☺ Not copy other people's work.

☺ Respect the privacy of files of other users. Only open and use the files that belong to you.

☺ Be polite and respect other people's views. The use of bad or inappropriate language or rude or aggressive behaviour is not allowed. This applies generally, but also in stored work, videos, e-mails, blogs, comments on the Learning Platform and on the school website.

☺ Allow your teacher, Head of School, Executive Headteacher or the ICT Staff to look at any material you store on the school network and the Learning Platform, this includes access your e-mails and uploaded documents.

☺ Not use portable storage devices, i.e. memory sticks, at school. Work can be emailed or uploaded onto the Learning Platform and accessed at school.

☺ Log off or shut down the computer when you have finished using it.

☺ Tell a member of staff if you see anyone breaking these rules. If you see any content on the Learning Platform which you are upset by tell staff by using the whistle blower tool.

☺ Tell a member of staff and use the whistle blower tool if you receive an unpleasant e-mail message. **DO NOT** delete it – your teacher of member of ICT staff will investigate it and delete it for you once they have dealt with the matter.

There is a copy of this policy on the School Website. Information on our School website is accessed using your email login and password.

There are consequences if you do not follow these rules. The Headteacher will be informed and a record will be kept of what has happened, and possibly one or more of the following:

☹ You may be banned from using the school network, internet, or accessing the Learning Platform and your email account.

☹ A letter will be sent telling your parents how you have broken the rules.

☹ The Headteacher of Parsons Down Junior School may give you a different punishment that they feel is appropriate.

This policy will be monitored by the ICT Coordinator and fully reviewed by the Full Governing Body annually.

Policy for the Acceptable Use of ICT, the School Network and Internet

I am signing to say that:

I understand and agree to follow the rules.
I understand what could happen if I break the rules.
I will tell a member of staff if I see anyone breaking these rules.

Child's Name (Please print) _____

Class _____

Signed _____

Parent/Carer Name (Please print) _____

Signed _____

Date _____

(Please sign and return to school)

E-Safety Rules

Think then Click

These rules help us to stay safe on the Internet

We only use and search the internet when an adult is with us

We can click on the buttons or links only when we know what they do.

We always ask an adult if we get lost on the Internet.

We open emails together with an adult.

We can write polite and friendly emails to people that we know.

Pupil's agreement

I understand the rules for using the computer.

I will always ask an adult for help using the computer so that I use it sensibly.

I know that adults will be able to see when I use the school's computers.

Signed / Marked…… Class ……

Child's Name……

Parent's Consent for Internet Access

I have read and understood the school e-safety rules and give permission for my son / daughter to access the internet. I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials but I appreciate that this is a difficult task.

I understand that the school cannot be held responsible for the content of materials accessed through the internet. I agree that the school is not liable for any damages arising from use of the internet facilities.

Please tick the box if you wish to have your child's username and password sent home. ☐

Signed ..... Date .....