Winwick C of E Primary School

e-Safety Policy

April 2013

Contents

Policy Control & Review

Policy Version

Version	Issue Date	Author	Distribution	Status	Approved Date
WeSP-V1.0 DRAFT	14th April 2013	A E Knight	Digital Committee	Draft	26th April 2013
WeSP-V1.0 DRAFT	21st April 2013	A E Knight	Headteacher & Staff	Draft	8th May 2013
WeSP-V1.0	9th May 2013	A E Knight	Governors	Final	13th May 2013

Policy Review

Action	Requirement
Reviewed by	Governing Curriculum Committee with the support of the e-Safety Coordinator and input from the Headteacher and Senior Management team as required.
Review Frequency	Annually
Review Date	Review date set by the Curriculum Committee and the review outcome and date of next review recorded in minutes of meeting.
Amendment	Should a change be required the Policy will be duly amended and re-issued. Brief details of the change shall be recorded within the 'Policy Change Control' appendix.
Issue	Electronic download (web site). Hardcopy on request.
Distribution	Staff, Governors, Parents.
Control	Uncontrolled upon download or printing.

Acknowledgement

This e-Safety policy is based on the Warrington School eSafety template document.

Source document:

Warrington School eSafety Policy 2010

Warrington Children and young people's Services

Nick Toyne, Senior Adviser, Chris Beedham, ICT Consultant, Chris Pennington, ICT Consultant.

School e-Safety Policy

New technologies have become integral to the lives of children in today's society, both within schools and in their lives outside school.

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children should have an entitlement to safe internet access at all times.

The requirement to ensure that children are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. Winwick's e-Safety policy should help to ensure safe and appropriate use.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement. However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to/loss of/sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing/distribution of personal images without an individual's consent or knowledge
- Inappropriate communication/contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video/internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this e-Safety policy is used in conjunction with other school policies (e.g. behaviour, anti-bullying and child protection policies).

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

Winwick must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. The e-Safety policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents/carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

Scope of the Policy

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

The Education and Inspections Act 2006 empowers headteachers, to such extent as is reasonable, to regulate the behaviour of 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 out of 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 roles and responsibilities for e-Safety 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 Curriculum Committee 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 designated e-Safety Co-ordinator
- regular monitoring of e-Safety incident logs
- reporting to relevant Governors committee/meeting

Headteacher

The Headteacher is responsible for ensuring the:

- safety (including e-Safety) of members of the school community
- e-Safety Coordinator and other relevant staff receive suitable 'Continuing Professional Development' (CPD) to enable them to carry out their e-Safety roles and to train other colleagues, as relevant
- monitoring and support of those in school who carry out the internal e-Safety monitoring role
- Senior Designated Person (SDP) for Safeguarding and Child Protection is aware of the procedures to be followed in the event of a serious e-Safety allegation being made against a member of staff

e-Safety Coordinator

The e-Safety Coordinator is responsible for:

- day to day responsibility for e-Safety issues and has a leading role in establishing and reviewing the school e-Safety policies/documents
- ensuring that all staff are aware of the procedures that need to be followed in the event of an e-Safety incident taking place
- provides training and advice for staff
- liaises with the Local Authority
- liaises with school ICT support services provider
- receives reports of e-Safety incidents and creates a log of incidents to inform future e-Safety developments
- meets regularly with e-Safety Governor to discuss current issues, review incident logs and filtering/change control logs
- attends relevant meeting/committee of Governors
- reports regularly to Senior Leadership Team

The e-Safety Coordinator is responsible for the management of the nominated School ICT service provider to ensure that:

- the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- that the school meets the e-Safety technical requirements
- that as appropriate the use of the network/Learning Platform is regularly monitored in order that any misuse/attempted misuse can be reported to the e-Safety Co-ordinator for investigation /action/sanction
- that monitoring software/systems are implemented and updated as agreed in school policies
- that systems and procedures fulfil the requirements of the protection of personal data

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 school Staff Acceptable Use Policy/Agreement (AUP)
- they report any suspected misuse or problem to the e-Safety Co-ordinator/Headteacher/Senior Leader/ for investigation/action/sanction.
- digital communications with pupils (email/Learning Platform) should be on a professional level.
- e-Safety issues are embedded in all aspects of the curriculum and other school activities
- pupils understand and follow the school e-Safety and acceptable use policy
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor ICT activity in lessons, extra-curricular and extended school activities
- they are aware of e-Safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices
- in lessons where internet use is pre-planned 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

Designated Child Protection Officer

Is responsible for liaising with the e-Safety co-coordinator concerning training in e-Safety issues and be aware of the potential for serious child protection issues to arise from:

- sharing of personal data
- access to illegal/inappropriate materials
- inappropriate online contact with adults/strangers
- potential or actual incidents of grooming
- cyber-bullying

Pupils

- are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy, which they will be expected to sign before being given access to school systems
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking/use of images and on cyber-bullying
- should understand the importance of adopting good e-Safety practice when using digital technologies out of school and realise that the school's e-Safety Policy covers their actions out of school, if related to their membership of the school

Parents/Carers

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website/Learning Platform and information about national/local e-Safety campaigns/literature. Parents and carers will be responsible for:

- endorsing (by signature) the Pupil Acceptable Use Policy
- accessing the school website/Learning Platform/online pupil records in accordance with the relevant school Acceptable Use Policy.

Community / Volunteer Users

Community / Volunteer Users who access school ICT systems/website/Learning Platform will be expected to sign a Community / Volunteer User AUP before being provided with access to school systems.

Policy Statements

Education – pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in e-Safety is therefore an essential part of the school's e-Safety provision. Children need the help and support of the school to recognise and avoid e-Safety risks and build their resilience. e-Safety education will be provided in the following ways:

- A planned e-Safety programme should be provided as part of ICT/PHSE/other lessons and should be regularly revisited
- Key e-Safety messages should be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities
- Pupils should be taught in all lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of information
- Rules for use of ICT systems/internet will be posted in all rooms

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 online experiences. Parents often either underestimate or do not realise how often children come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it.

Winwick will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters, web site, learning platform
- Parents' evenings

Education & Training – Staff

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. An audit of the e-Safety training needs of all staff will be carried out regularly.
- 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 Policies
- The e-Safety Coordinator will receive regular updates through attendance at LA/other information/training sessions and by reviewing guidance documents released by WBC and others
- This e-Safety policy and its updates will be presented to and discussed by staff in staff/team meetings/INSET days
- The e-Safety Coordinator will provide advice/guidance/training as required to individuals as required

Training – Governors

Governors should take part in e-Safety training/awareness sessions, with particular importance for those who are members of any committee/group involved in ICT/e-Safety/health and 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, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible.

- School ICT systems will be managed in ways that ensure that the school meets the e-Safety technical requirements outlined by the Acceptable Usage Policy.
- School ICT systems will be regularly updated to ensure up-to-date anti-virus definitions and Microsoft Windows Security Updates are installed.
- There will be regular reviews and audits of the safety and security of school ICT systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- The network will be managed such that Staff and Pupil areas are segregated and secure.
- Staff network access rights will be determined by the individuals teaching / management needs.
- Staff will be provided with individual user login credentials, the frequency of changes to password being at the user's discretion.
- Guest logins will be created for visitor, trainee teacher temporary access to the school network.
- Pupil users will be provided with a class shared year group user name and password for access to the school network and internet.
- All users of the school learning platform will be provided with a username and password for secure access in school and beyond.
- The "master/administrator" passwords for the school ICT system will be kept secure with restricted access.
- School Data should be securely managed when taken off the school site using encrypted memory devices or password protected files.
- Personal data held by the school and data important to the running and continuity of teaching will be securely backed up.
- The school maintains and supports a managed filtering service blocking inappropriate websites. This Service provides security – Anti-Virus, Intrusion Prevention and Anti-Phishing arising from website pages being visited.

Curriculum

e-Safety should be a focus in all areas of the curriculum and staff should reinforce e-Safety messages in the use of ICT across the curriculum.

- e-Safety should be taught regularly through a scheme of work with identified progression of knowledge, skills and understanding.
- e-Safety skills should be embedded through both discrete ICT and cross-curricular application.
- In lessons where internet use is pre-planned, it is best practice that 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 pupils are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites visited.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

Use of digital photographic and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet.

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.
- Staff 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. However should circumstances require, with the express permission of the Headteacher, images may be taken on staff owned equipment provided that at the first available opportunity they are transferred to the school's network / Learning Platform and deleted from the staff device.
- Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.

Data Protection

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

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, USB stick or any other removable media:

- the data must be encrypted and password protected
- the device must be password protected (many memory sticks/cards and other mobile devices cannot be password protected)
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device once it has been transferred or its use is complete

Communications

When using communication technologies the school considers the following as good practice:

- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and pupils or parents/carers (email, chat, Learning Platform etc.) must be professional in tone and content. Pupil communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat/social networking programmes must not be used for Pupil communications.
- Pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.

Unsuitable/inappropriate activities

The school believes that the activities referred to in the following section would be inappropriate in a school context and those 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 certain internet usage as follows:

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 any illegal material or any other information which breaches the integrity of the school ethos, offends school colleagues or has the potential to bring the school into disrepute.
- Use school systems to run a private business.
- Knowingly bypass school system filtering without documented permission.
- Upload, download or transmit commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions.
- Reveal or publicise confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords).
- Create or propagate computer viruses or other harmful files.
- Carry out sustained or instantaneous high volume network traffic (downloading/uploading files) that causes network congestion and hinders others in their use of the Internet
- Engage in online gambling or gaming.

Responding to incidents of misuse

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If any apparent or actual misuse appears to involve illegal activity i.e.

- child sexual abuse images
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

The Appendix 'Incident Reporting' should be consulted and actions followed in line with the flow chart, in particular the sections on reporting the incident to the police and the preservation of evidence.

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation.

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.

Incidents of misuse will be recorded and managed using the form 'ICT Incident of Misuse Report'.

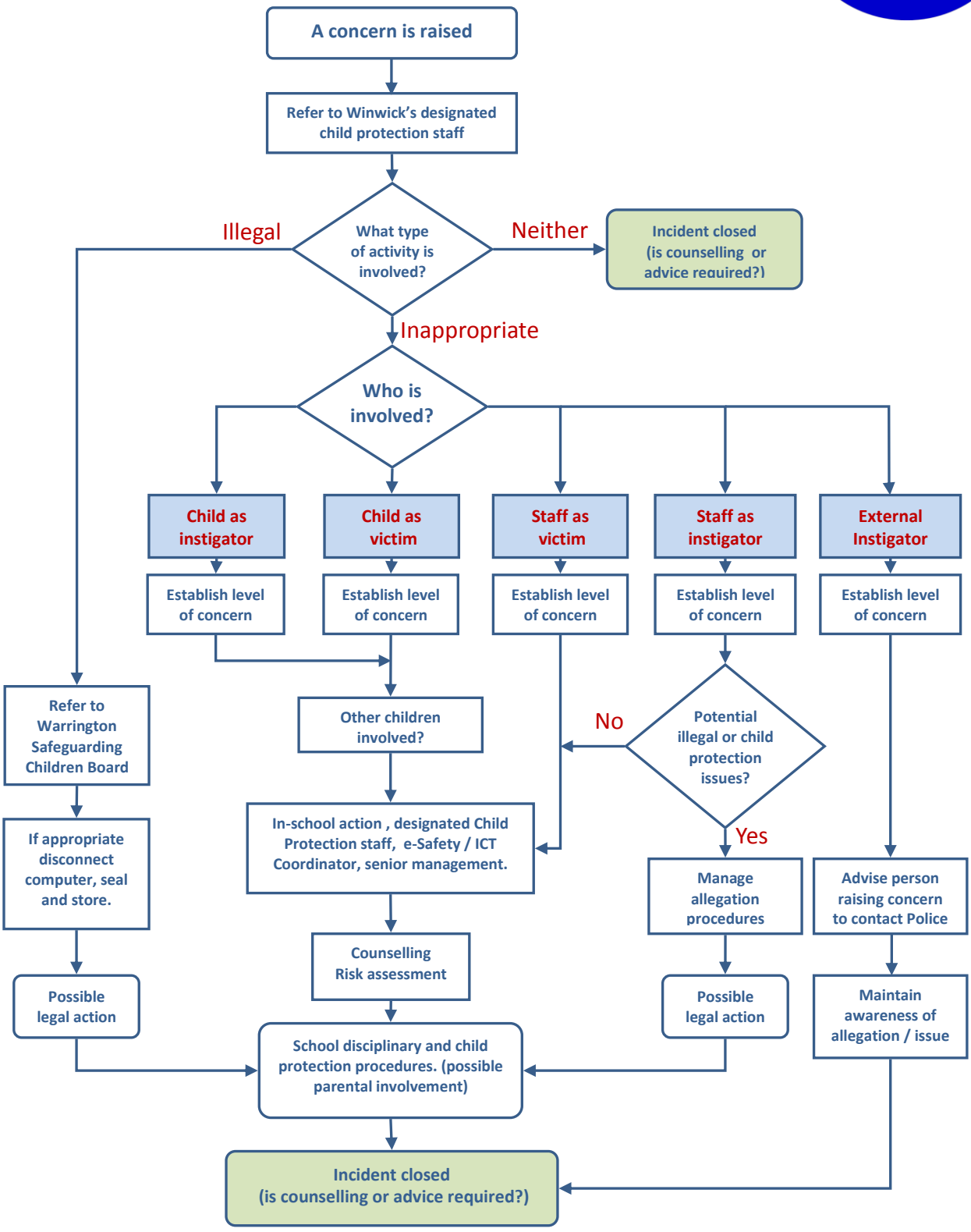
Parent e-Safety Information Pack

Each Parent / Carer will be issued with an information pack containing the following documents:

- e-Safety Cover Letter
- Parents /Carers Acceptable Usage Policy
- Pupil Acceptable Usage Policy
- Parents – Keep Your Child e-Safe!

Appendices

Incident Reporting



Pupil Acceptable Use Policy

Parent / Carer Information

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning.

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

The school will try to ensure that pupils will have good access to ICT to enhance their learning and will, in return, expect the pupils to agree to be responsible users.

Responsible Use

The 'Rules for Responsible Computer and Internet Use' are those that Winwick School consider to be responsible child behaviour when using ICT equipment and accessing the Internet both in school and at home. It is recognised that depending upon the age of your child certain statements will be more relevant than others. Please consider these statements and discuss those that are most appropriate to your child's level of comprehension and understanding before signing the 'Pupil Acceptable Use Policy' Agreement. Each year your child will receive e-Safety reinforcement input in class. In addition to this as your child's Internet awareness develops please take the opportunity to reinforce and develop the safe and responsible use messages below.

e-Safety

In order to ensure that your child understands the guidelines for the safe use of the Internet while in school and at home please discuss and explain the 'Rules for Responsible Computer and Internet Use' with your child. To focus your discussion please use the attached KS1 and KS2 e-Safety Internet Rules leaflets as appropriate with your child. It is recommended that you stick the chosen leaflet in a visible place in your home and from time to time take the opportunity to direct your child's attention to it and reinforce the rules with them.

On the Winwick web site you will find an e-Safety section. Please explore this and look at the appropriate KS1 or KS2 video clips and texts with your child. From the Winwick web site you will also be able to download view and print a larger version of the KS1 and KS2 e-Safety Rules leaflets. The e-Safety Policy is also available for download from this section of Winwick's web site.

Please note in order for your child to access the internet whilst in school, this user agreement must be returned fully and positively completed and signed to the school. Please help your child if necessary to sign the agreement and if they are unable to sign it then please sign it for them. Then please also sign the return slip to confirm that you have discussed the rules with your child and together you have looked at the e-Safety information and videos on Winwick's website.

Please note: You will need to complete a separate 'Pupil Acceptable Use Policy Agreement' slip for each of your children. Should you require additional slips these may be obtained from the school office or you may photocopy the attached blank slip as required.

Rules for Responsible Computer and Internet Use

- I will ask permission before using the Internet.
- I will not try to harm any equipment or the work of another person on a computer.
- I will only look at or delete my own files.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty.
- If I find something that I think I should not be able to see, I must tell my teacher or parents straight away and not show it to other pupils.
- I must not write anything that might upset someone or give the school a bad name.
- The messages I send will be polite and responsible and never aggressive or hurtful (bullying).
- I must not tell anyone my name, where I live, or my telephone number - over the Internet.
- I will never arrange to meet anyone I don't know.
- I will only email people I know.
- I will not open emails sent by anyone I don't know.
- I will not use Internet chat rooms.
- I must not tell my username and passwords to anyone else but my parents.
- If I think someone knows my password I will tell a teacher.
- I must never use other people's usernames and passwords or computers left logged in by them.
- I must log off after I have finished with my computer.
- I will never download files without permission from a teacher as this may harm our computer network.
- I will not use work from the Internet as if it was my own.
- I know that the teachers will regularly check what I have done on the school computers.
- I understand that if I break these rules, I may not be allowed to use the Internet or computers.
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.

KS1-Keep Safe!

My Rules

To help me to stay safe on the Internet

I will only use the Internet when an adult is with me.

I can click on the buttons or links when I know what they do.

I can search the Internet with an adult.

I will always stop and ask if I get lost on the Internet.

I can open and write polite and friendly emails to people that I know.

KS1 e-Safety - Winwick C of E School - 2013

Words adapted from - B. Stoneham & J. Barrett

KS2-Keep Safe!

My Rules

To help me to stay safe on the Internet

- ☺ **I** will ask permission before using the Internet.
- ☺ **I** only use websites that an adult has chosen.
- ☺ **I** will tell an adult if I see anything I am uncomfortable with.
- ☺ **I** will immediately close any webpage I am not sure about.
- ☺ **I** will only email people I know.
- ☺ **I** will not open emails sent by anyone I don't know.
- ☺ **I** will send emails that are polite and friendly.
- ☺ **I** will never arrange to meet anyone I don't know.
- ☺ **I** will never give out personal information or passwords.
- ☺ **I** will not use Internet chat rooms.
- ☺ **I** will never share my passwords.

KS2 e-safety - Winwick C of E School - 2013

Your Child – Data Protection

Under the "Fair Processing" requirements in the Data Protection Act, Winwick School is required to inform parents/carers of all data they hold on their child, the purposes for which the data is held and the third parties to whom it may be passed.

Winwick School processes personal data about its pupils and is a "data controller" in respect of this for the purposes of the Data Protection Act 1998. It processes this data to:

- support its pupils' teaching and learning
- monitor and report on their progress
- provide appropriate pastoral care
- assess how well the school as a whole is doing

This information includes contact details, national curriculum assessment results, pupil progress records, reports, attendance information, characteristics such as ethnic group, special educational needs, any relevant medical information and any other information that might be disclosed by parents/carers or by other agencies working with families or staff members.

From time to time the school is required to pass on some of this data to local authorities, the Department for Children, Schools and Families (DCSF), and to agencies that are prescribed by law, such as the Qualifications and Curriculum Authority (QCA), Ofsted, the Learning and Skills Council (LSC), the Department of Health (DH), Primary Care Trusts (PCT). All these are data controllers for the information they receive. The data must only be used for specific purposes allowed by law.

Further information on the organisations that may receive data and how this data is used can be found on Winwick's web site www.winwick.eschools.co.uk

Please retain this document for your information.

Your child will not be allowed to use the school ICT systems until the slip below is received fully and positively completed.

Please complete all tick boxes and the form, then cut along the dotted line and return the signed slip to your child's Class teacher.

Pupil Acceptable Use Policy Agreement

- My Parent / Carer has explained the 'Rules for Responsible Computer and Internet Use' to me and we have read the 'e-Safety Rules'.
- We have looked at the information and videos on the e-Safety section of the school's web site.
- We have talked about how important it is for me to always remember to use these Rules when I am using the Internet and email in school or at home.

I know that if I get lost on the internet or see anything that I am uncomfortable with I must tell an adult straight away. I will always follow the rules and understand that these rules will help me to keep safe.

Pupil Name		Parent/Carer Name	
Signed		Signed	
My Year is		Date	

Well done now return this signed form to your teacher.

Staff (and Volunteer) AUP

Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that pupils receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-Safety in my work with young people.

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (eg laptops, email, learning platform etc) out of school.
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
- I will ensure that I log-out in order to prevent any potential security breach resulting from unauthorised users using my log-in credentials.
- I will ensure that any computer I use locks within 5 minutes of inactivity and requires a password to re-gain access.
- I will immediately report any illegal, inappropriate or harmful material or incident; I become aware of, to the appropriate person.
- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images. I will not use my personal equipment to record these images, unless I have permission to do so.
- Images shall only be published if the pupil's parent/carer has given permission by the return of the Parent AUP. Where general individual or group pupil images are published (e.g. sports day, school trips etc.), it will not be possible to identify by name, or other personal information, those who are featured. Should an image be associated with celebrating the school's or pupil's success (e.g. competition winner, school award etc.) then the name of the pupil may be published.
- I will only use chat and social networking sites in school in accordance with the school's policies.
- I will only communicate with pupils and parents/carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any online activity that may compromise my professional responsibilities.
- When I use my personal hand held/external devices (includes but is not exclusive to the following types:- PDAs, laptops, mobile phones, USB devices) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.

- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will ensure that my data is regularly backed up.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Personal Data Holding Policy. Where personal data is transferred outside the secure school network, it must be encrypted.
- I understand that data protection policy requires that any staff or pupil data, to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will ensure that where personal data is held in hardcopy format, whilst in my possession I will keep it safe, secure (under lock and key) and ensure that it is returned as soon as practicably possible to the School Office for safe keeping.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).
- I understand that I am responsible for my actions in and out of school.
- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and / or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff/Volunteer Name	
Signed	
Date	

Parent / Carer AUP

This AUP remains active for the duration of your child's attendance at Winwick School, should you wish to make any future amendment to your consent please write to the school.

Acceptable Use Policy (AUP) – Permission Form

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning.

In order for your child to be able to use the School ICT systems and / or the School to take and use pictures of your child you are required to sign and return this permission form.

Parent/Carers Name		Pupil Name		Year	

Use of ICT systems **(complete if you would like your child to use the school's ICT systems)**

As the parent/carer of the above pupil, I give permission for my son/daughter to have access to the internet and to ICT systems at school.

I know that my son/daughter has signed an Acceptable Use Agreement and has received, or will receive, e-Safety education to help them understand the importance of safe use of ICT – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's/daughter's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's e-Safety.

Signed		Date	

Use of Digital/Video Images **(complete if you are happy for your child's photograph to be used)**

The use of digital/video images plays an important part in learning activities. Pupils and members of staff may use digital cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons. Images may also be used to celebrate success or a school event through their publication in newsletters, on the school website and occasionally in the public media. Group pictures (school outings, classroom work etc.) will usually be anonymous; however in situations to celebrate your child's success (e.g. competition winner, school award etc.) their name and image may be published.

As the parent/carer of the above pupil, I agree to the school taking and using digital/video images of my child/children. I understand that the images will only be used to support learning activities or in publicity that reasonably celebrates success and promotes the work of the school.

I agree that if I take digital or video images at, or of, school events which include images of children, other than my own, I will abide by these guidelines in my use of these images.

Signed		Date	

Please return the complete form signed where appropriate to your child's class teacher.

Parents – Keep Your Child e-Safe!

Whilst in school your child will be using ICT systems that focus on so far as practicably possible filtering content that could be considered offensive or illegal, but what about at home?

What are you doing to protect your child?

How many parents encourage their children to use child friendly search engines or have altered/configured their home computers to filter content such that it is suitable for children's eyes? If you have not already done so then please read on.

Safekids.co.uk has much information on all aspects of keeping your child safe and particularly good advice on how to help keep your child safe when using the computer and internet from home. Please visit the Safekids web site (www.safekids.co.uk) for everything you are likely to need to know. In the meantime an extract from one of their articles is copied below:

Which Search Engines are Safe for Kids?

There are a number of search engines which offer child-friendly content only. They achieve this by filtering out inappropriate content which you, as a parent, would find offensive for your child. In general, this is achieved by using human beings to filter out the unsuitable sites.

The filtered sites include those which address explicit sexual matters, pornography, violence, drug use, and gambling etc.

Below is a summary of some of the most popular child friendly search engines:

Ask Jeeves for Kids

It is designed to be a kid-friendly way for children to search online with a focus on learning and educational entertainment. Ask for Kids uses natural-language technology that allows kids to ask questions and perform web searches, such as "When did Hawaii become a state?" or "What's it like to live in space?" or even "Convert 122 inches into feet" in the same way they would ask a parent, friend or teacher.

Yahoo Kids!

www.kids.yahoo.com – the Yahoo for kids is designed for ages 7 to 12. All of the sites are hand-picked to be appropriate for children. Also, unlike normal Yahoo, searches will not bring back matches found by crawling the web, if there is no match from within the Yahooligan listings. This prevents possibly objectionable sites from slipping onto the screen.

Filtering Options

Most major search engines including Google, Yahoo (in the main) and MSN obtain their listings by crawling the web and then using advance techniques to determine search results. The fact there is no human review and categorisation, as with the child-friendly sites listed above, means it's easy for undesirable material to appear in search results.

As a solution, most major search engines offer the ability to filter the results to keep out pornography and other material that you would not want your children to encounter. Below are some tips on enabling child safe filtering in major search engines:

Google: Go to the Google Home Page, select Preferences (on the right of the search box) and in the SafeSearch Filtering section select the option for 'Use strict filtering (Filter both explicit text and explicit images)'.

MSN Search: Use the Safe Search Filter on the Settings page.

Yahoo: Set the SafeSearch Filter option via the Search Preferences page.

AltaVista: Use the Family Filter Setup page.

AOL Search: Doesn't appear to offer a filter, but enabling Parental Controls might have an impact on web search matches.

Ask Jeeves: Use options for Content Filtering on the Your Settings page or try Ask For Kids.

Lycos: Use the Adult Filter section of the Advanced Search Filters page.

Filtering and Blocking Software

One alternative option is filtering software which works across the entire web, not just for search results. Most filtering software provides a decent level control for parents to determine what it and is not allowed for the kids to see. CyberPatrol and NetNanny are two of the most widely used programs for this type of control.

This article may be found at:
www.safekids.co.uk/ChildFriendlySearchEngines.html

e-Safety Incident of Misuse Report

Form to be maintained electronically by the e-Safety Coordinator.

Incident Date	Reported by	Brief description of alleged misuse	User(s) involved	Year Group	Names of Investigators	Brief description of findings and outcome	Date of closure	Report completed by

School Filtering Policy

Introduction

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so. It is therefore important that the school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.

As a part of the North West Grid for Learning (NWGfL) schools and connected organisations automatically receive the benefits of a managed filtering service, with some flexibility for changes at local level.

Responsibilities

The responsibility for the management of the school's filtering policy will be held by the e-Safety Coordinator. They will manage the school filtering, in line with this policy and will keep records/logs of changes and of breaches of the filtering systems.

To ensure that there is a system of checks and balances and to protect those responsible, changes to the Warrington/school filtering service must:

- be logged in change control logs
- be reported to a second responsible person (Headteacher)

All users have a responsibility to report immediately to the e-Safety Coordinator any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.

Users must not attempt to use any programmes or software that might allow them to bypass the filtering/security systems in place to prevent access to such materials.

Education/Training/Awareness

Pupils will be made aware of the importance of filtering systems through the e-Safety education programme. They will also be warned of the consequences of attempting to subvert the filtering system.

Staff users will be made aware of the filtering systems through:

- signing the AUP
- induction training
- staff meetings, briefings, Inset

Parents will be informed of the school's filtering policy through the Acceptable Use agreement.

Changes to the Filtering System

Users who gain access to, or have knowledge of others being able to access, sites which they feel should be filtered (or unfiltered) should report this in the first instance to (insert title) who will decide whether to make school level changes (as above). If it is felt that the site should be filtered (or unfiltered) at Warrington level, the ICT Coordinator should contact the ICT Help Desk with the URL.

Requests for changes to the School filtering policy will be managed and authorised electronically. The audit trail of emails and authorisation will be maintained by the e-Safety Coordinator.

Record of Change to Filtering System

Form to be maintained electronically by the e-Safety Coordinator.

Request Date	Requestor	Request to unblock URL / web address (include details of reason for lifting restriction)	Request reviewed by	Date Request approved by Headteacher

School Password Security Policy

Introduction

The school will be responsible for ensuring that the school network is as safe and secure as is reasonably possible and that:

- users can only access data to which they have right of access
- access to personal data is securely controlled in line with the school's personal data policy
- logs are maintained of access by users and of their actions while users of the system

An appropriate username/password system will be established and will apply to all school ICT systems, including email and Learning Platform.

Responsibilities

The management of the password security policy will be the responsibility of ICT Coordinator.

Staff must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.

Pupils will access the school network through shared year group passwords. Pupils must only use the password for their year group. Staff must be vigilant of this during lessons which include access to the school network and internet.

Passwords for new users and replacement passwords for existing users will be arranged by the ICT Coordinator through liaison with the schools ICT service provider.

Training/Awareness

Members of staff will be made aware of the school's password policy:

- at induction
- through the school's e-Safety policy and password security policy
- through the Acceptable Use Agreement

Pupils will be made aware of the school's password policy:

- in ICT and/or e-Safety lessons
- through the Acceptable Use Agreement

See related Appendix - ICT Network Infrastructure Set-up.

ICT Network Infrastructure Set-up

It is the responsibility of the ICT Coordinator to ensure that the services described below or alternatives, together with any additional services that may be required but not listed are renewed in sufficient time to maintain continuity of service cover and support.

Requirement	Implementation
ICT Service Provider	EDAC Abacus House, 450 Warrington Road, Culcheth, Warrington, WA3 5QX Tel 01925 572573/596157, Fax 08717 146713 Contact: Nigel Spencer nigel@edac-solutions.co.uk
Internet Access and Filtering	Winwick subscribe to Warrington Borough Council for the 'Warrington Internet Access for Schools' service. Comprising of: • Web Filtering – blocking of inappropriate websites. • Security – Anti-Virus, Intrusion Prevention, Anti-Phishing. • Scalable Bandwidth • Mail Relay Services Liability – misuse resulting in liability resides with Local Authority. Should Warrington's monitoring systems reveal a misuse the School will be informed of this and the occurrence will be reviewed accordingly.
Virus & Malware Protection	Sophos Endpoint, automatic updates. Additionally the ICT Service Provider receives updates from WBC of any alerts such as port spamming and Malware traffic which allows the potential threat to be addressed quickly.
Data Backup	Redstore on-line backup service used. Off-site backup to Redstore secure servers. Redstore responsible for security and integrity of backups. The ICT Service Provider is responsible for reviewing Redstore email notification of backup status in order to ensure that backups are taking place and successful.
Data Restoration	Should it be necessary to restore data, the ICT Service Provider will assist the ICT Coordinator in determining the root cause of the loss of data and if necessary the ICT Coordinator will introduce procedures to prevent / reduce the risk of a similar future occurrence. The ICT Service Provider will access the remote back-up and perform a restoration in order to re-create / repair any lost or corrupted data to its original state.

Administration Data Backup	Staff personal data, SIMS, FMS maintained by Warrington school support. Warrington responsible for backup, integrity and safety of administration data.
Protection of Personal Data	Personal date maintained on Network G drive. G drive only available to Headteacher and Office Staff. Physical segregation to curriculum network. Access to the Admin system is restricted by User name and password, with the passwords prompting to be changed every 42 days, in line with WBC policy and Microsoft Guidelines. Authorised user machines are part of WLA domain and access authenticated by Warrington servers. The Schools MIS System, SIMS, hold all the pupil and staff Personal data, and access to this system is again further restricted by user name and password. Access to SIMS is also controlled so that staff have different levels of access so that they only see relevant information. There is also an Audit log within SIMS so that the System Manager would be able to see who and what area of SIMS has been accessed. The Audit log provides details of user activity by recording: Date, Log in name, User name, Access Area, Action, Scope, Module, workstation.
Staff User Passwords	The ICT Service Provider will generate login credentials and upon the request of the ICT Coordinator re-set these passwords if necessary. Staff will be required to choose their own passwords on first log-in, thereafter staff shall ensure that they log-out after each session in order to prevent any potential security breach.
Guest User Passwords	The ICT Service Provider will generate login credentials and upon the request of the ICT Coordinator re-set these passwords if necessary. The ICT Coordinator will issue the Guest with User credentials for the time required whilst in school. Guest user access will be restricted to internet access only. Should a Guest require extended access for more than 5 days and/or require additional network access rights the ICT Coordinator will request a login from the ICT Service Provider and the Guest will be assigned a temporary account as if 'Staff'. As soon as the Guest is no longer in need of access the ICT Coordinator will ensure that the account is suspended.
Pupil User Passwords	The ICT Service Provider will generate Class/Year group logins. These login credentials will remain fixed. The class teacher will be vigilant to ensure that the class uses the correct year group login.

Web Site / Learning Platform	The School Learning Platform is provided by: eSchools. www.eschools.co.uk 0845 557 7056
Learning Platform Passwords	User passwords (Teachers, Pupils, Parents and Governors) will be issued by eSchools upon request of the ICT Coordinator. Passwords will be issued to user groups by the ICT Coordinator. The ICT Coordinator will as required liaise with eschools to arrange for the re-setting of passwords should this be required. The ICT Coordinator will manage day to day password management through the Learning Platform administration function.
Web Site / Learning Platform Backup	The Learning Platform servers are hosted remotely and subject to 24 hour monitoring and back up on a regular basis. For resilience all of the Learning Platform content is copied to multiple servers to protect against loss of service. Should a problem be experienced with the Learning Platform it is through eSchools possible to roll-back to a previous version (within 7 days) and so restore the functionality and operation of the Learning Platform.
Network Segregation	The Network Staff and Pupil data storage areas will be segregated.
Pupil Network Data Structure	Each class will have a dedicated data folder which will only be accessible by that class. The Class folder will be named after the year group eg Year 6. Each pupil will have a named folder within the class folder. The teacher will be vigilant that each child only accesses their own folder and is respectful of other pupil's folders. At the end of the academic year the ICT Coordinator in liaison with the ICT Service Provider will copy the pupil directory and all data to 'Archive' and rename it by appending the academic year for identification if so required (OFSTED). From the original Pupil folder structure each class folder will be renamed in order to migrate it's users to the new academic year and all existing data will be purged. The new reception class intake will have a new class folders created for it. Permissions to a Pupil Year folder: Class Pupils, The year teacher, Headteacher, All Coordinator roles.
Staff Network Data Structure	Each class teacher will have a dedicated data folder named after the class eg Year 6. Permissions to Teacher folders: The year teacher, Headteacher, All Coordinator roles. Share area - this will be a dedicated folder accessible by all teachers for the sharing of common resources.
Archive	Assuming that Network storage capacity is not limited the Archive folder will be reviewed annually and all data older than the last academic year purged.

Network Hierarchy	

Network Hierarchy format – example Year 6			
PUPILS			
	Year 6		
		pupil.name	
			User defined
TEACHER			
	Year 6		
		Subjects	
			User defined
		Media	
			Photos
			Videos
			Music
		General	
SHARE			
	Subjects		
		Year 6	
			User defined
	Media		
		Photos	
			Year 6
		Videos	
			Year 6
		Music	
			Year 6
	General		
	Archive		

School Personal Data Handling Policy

Introduction

It is the responsibility of all members of the school community to take care when handling, using or transferring personal data that it cannot be accessed by anyone who does not:

- have permission to access that data
- need to have access to that data.

Any loss of personal data can have serious effects for individuals and/or institutions concerned, can bring the school into disrepute and may well result in disciplinary action and/or criminal prosecution. All transfer of data is subject to risk of loss or contamination.

The Data Protection Act (1998) lays down a set of rules for processing of personal data (both structured manual records and digital records). It provides individuals (data subjects) with rights of access and security and requires users of data (data processors) to be open about how it is used and to follow "good information handling principles".

Policy Statements

The school will hold the minimum personal information necessary to enable it to perform its function and information will be erased once the need to hold it has passed.

Every effort will be made to ensure that information is accurate, up to date and that inaccuracies are corrected without unnecessary delay.

All personal data will be fairly obtained in accordance with the "Fair Processing Code" and lawfully processed in accordance with the "Conditions for Processing".

Personal Data

The school and individuals will have access to a wide range of personal information and data. The data may be held in digital format or on paper records. Personal data is defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances. This will include:

- Personal information about members of the school community – including pupils, members of staff and parents and carers eg names, addresses, contact details, legal guardianship/contact details, health records, disciplinary records
- Curricular/academic data eg class lists, pupil progress records, reports, references
- Professional records eg employment history, taxation and national insurance records, appraisal records and references
- Any other information that might be disclosed by parents/carers or by other agencies working with families or staff members

Responsibilities

Everyone in the school has the responsibility of handling protected or sensitive data in a safe and secure manner.

Governors are required to comply fully with this policy in the event that they have access to personal data, when engaged in their role as a Governor.

Registration

The school is registered as a Data Controller on the Data Protection Register held by the Information Commissioner.

Information to Parents/Carers – the "Fair Processing Notice"

Under the "Fair Processing" requirements in the Data Protection Act, the school will inform parents/carers of all pupil data they hold on the pupils, the purposes for which the data is held and the third parties to whom it may be passed. This fair processing notice will be passed to parents/carers as part of their Child's Pupil Acceptable Use Policy agreement.

Training & awareness

All staff will receive data handling awareness/data protection training and will be made aware of their responsibilities, as described in this policy through:

- Induction training for new staff
- Staff meetings/briefings/Inset

Secure Storage of and access to data

The school will ensure that ICT systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them.

Personal data may only be accessed on machines that are securely password protected. Any device that can be used to access data must be locked if left (even for very short periods) and set to auto lock if not used for five minutes.

All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.

Personal data can only be stored on school equipment (this includes computers and portable storage media) Private equipment (ie owned by the users) must not be used. When personal data is stored on any portable computer system, USB stick or any other removable media:

- the data must be encrypted and password protected
- the device must be password protected (many memory sticks/cards and other mobile devices cannot be password protected)
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

The school has clear policy and procedures for the automatic backing up, accessing and restoring all data held on school systems, including off-site backups.

Secure transfer of data and access out of school

The school recognises that personal data may be accessed by users out of school, or transferred to the LA or other agencies. In these circumstances:

- Users may not remove or copy sensitive or personal data from the school or authorised premises without permission and unless the media is encrypted and password protected and is transported securely for storage in a secure location.
- Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (eg family members) when out of school.
- When data is required by an authorised user from outside the school premises (for example, by a teacher or a contractor) they must have secure remote access to the management information system (MIS) or learning platform.
- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software.

- Particular care should be taken if data is taken or transferred to another country, particularly outside Europe, and advice should be taken from the local authority in this event.

Hardcopy data

- Where data is held in paper hardcopy format, this will be kept safe and secure by the holding individual.
- The paper hardcopy document will be returned as soon as practicably possible to the School Office.
- The paper hardcopy document will be stored in a locked filing cabinet within the School Office.

Disposal of data

The school will comply with the requirements for the safe destruction of personal data when it is no longer required.

The disposal of protected data, in either paper or electronic form, must be conducted in a way that makes reconstruction highly unlikely. Electronic files must be securely overwritten, in accordance with government guidance and other media must be shredded, incinerated or otherwise disintegrated for data.

Audit Logging/Reporting/Incident Handling

As required by the "Data Handling Procedures in Government" document, the activities of data users, in respect of electronically held personal information, will be logged and these logs will be monitored by a designated member of Office staff and/or Headteacher.

The audit logs will be kept to provide evidence of accidental or deliberate security breaches – including loss of protected data or breaches of an acceptable use policy, for example. Specific security events should be archived and retained as evidential quality for seven years.

The school policy for reporting, managing and recovering from information risk incidents is managed through the use of the 'School Personal Data Misuse' form, which establishes:

- a "responsible person" for each incident
- a communications plan, including escalation procedures
- and results in a plan of action for rapid resolution and
- a plan of action of non-recurrence and further awareness raising.

All significant data protection incidents must be reported to the Information Commissioner's Office based upon the local incident handling policy and communication plan.

In the event of a potential data protection issue the 'School Personal Data Misuse Report' form will be used. This form will provide an audit trail for the recording, investigating, escalation and plan for recovery from a potential information risk incident.

School Personal Data Misuse Report

In the event of potential misuse, mistaken distribution of or loss of personal data this form will be completed by the designated personal data System Manager and immediately escalated to the Headteacher. Each incident will be recorded on a new form.

Investigating System Manager (name)	
Investigation	
Date of misuse / issue incident	
Outline description of misuse / issue	
Details of activity from records of audit log	
System Manager conclusion and recommendations	
Date of completion of Investigation	
Escalation	
Meeting Date with Headteacher	
Headteacher comments / input	
Agreed Actions	
Requirements to escalate to external body	
Communication / Resolution plan	
Actions to prevent re-occurrence	
Reinforcement / Awareness training	
Headteacher confirmation of action completion and close down of incident	
Signed:	Date:

Policy Change Control

Version	Brief Details of Change
WeSP-V1.0	Initial Release

Winwick CE Primary School
Myddleton Lane
Winwick
Warrington
WA2 8LQ