Glazebury C E Primary School

Policy Header

Policy Title	**E-Safety Policy**
Version No	**3**
Written / Adopted Date	**Written Feb 2016** **Reviewed March 2016** **Reviewed March 2017**
This policy complies with WBC guidance	
Linked Policies	**Behaviour, Bullying, Curriculum.**
Written By	**Mrs. J Hindley** **Mr. P Snelson**
Date shared with Staff	**April 2018**
Date Ratified by Governors	**25/04/17**
Review Date	**April 2018**

Rationale;

E-Safety encompasses the use of new technologies, internet and electronic communications such as mobile phones, collaboration tools as well as those more regularly thought of such as computers, laptops and tablet devices. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

The previous “E-Safety Commitment” has been extensively revised and will now be named the Schools’ e-Safety Policy to reflect the need for us to further raise awareness of the safety issues associated with electronic communications as a whole.

As with all other potential risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build students’/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.

We, as a school must demonstrate that we have provided the necessary safeguards to help ensure that we have done everything that could reasonably be expected to manage and reduce these risks. The eSafety 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.

The school’s e-safety policy will operate in conjunction with other policies including (but not limited to), those for Student Behaviour, Bullying, and curriculum

Purpose;

- Ensure that children and young people are able to use the internet and related communications technologies appropriately and safely
- A school eSafety policy should help to ensure safe and appropriate use.
- To involve all stakeholders in the develop and implementation a safe usage strategy
- To use exciting and innovative tools in school and at home to raise educational standards and promote pupil/student achievement.
- To educate pupils against the dangers of the usage of new technologies that could 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.

Scope;

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 school ICT systems, both in and out of school. The Education and Inspections Act 2006 empowers head teachers, 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 eSafety 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.

Roles and Responsibilities;

The following section outlines the roles and responsibilities for eSafety of individuals and groups within the school:

Governors:

Governors are responsible for the approval of the eSafety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors' Education Sub Committee receiving regular information about eSafety incidents.

Head teacher and Senior Leaders:

• The Head teacher is responsible for ensuring the safety (including eSafety) of members of the school community, though the day to day responsibility for eSafety will be delegated to the eSafety Coordinator. At this time (Sept 14) the eSafety Coordinator is the ICT Coordinator.

• The Head teacher/Senior Leaders are responsible for ensuring that the ICT Coordinator and other relevant staff receive suitable CPD to enable them to carry out their eSafety roles and to train other colleagues, as relevant.

• The Head teacher/Senior Leaders will support those in school who carry out the internal eSafety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

• The Head teacher and another member of the Senior Leadership Team/Senior Management Team should be aware of the procedures to be followed in the event of a serious eSafety allegation being made against a member of staff. (see WBC flow chart on dealing with eSafety incidents – included in a later section – "Responding to incidents of misuse" and relevant Local Authority HR/disciplinary procedures).

Designated eSafety Coordinator:

- Reports to the safeguarding committee.
- Takes day to day responsibility for eSafety issues and has a leading role in establishing and reviewing the school eSafety policies/documents.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an eSafety incident taking place.
- Provides training and advice for staff.
- Liaises with the Local Authority.
- Liaises with school ICT technical staff.
- Receives reports of eSafety incidents and creates a log of incidents to inform future eSafety developments.
- Meets regularly with eSafety Governor to discuss current issues, review incident logs and filtering/change control logs (Safeguarding Committee).
- Reports regularly to Senior Leadership Team.

Network Manager/Technical staff:
The Network Manager is responsible for ensuring:

- that the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- that the school meets the eSafety technical requirements as advised by Becta and the Acceptable Use Policy.
- the school's filtering policy , is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that they keeps up to date with eSafety technical information in order to effectively carry out their eSafety role and to inform and update others as relevant
- that the use of the network/Learning Platform/remote access/email is regularly monitored in order that any misuse/attempted misuse can be reported to the safeguarding committee for investigation/action/sanction
- that monitoring software/systems are implemented and updated as agreed in school policies

Teaching and Support Staff;
are responsible for ensuring that:

- they have an up to date awareness of eSafety matters and of the current school eSafety policy and practices
- they have read, understood and signed the school Staff Acceptable Use Policy (AUP)
- they report any suspected misuse or problem to the eSafety Co-ordinator/Head teacher/Senior Leader for investigation/action/sanction
- digital communications with students/pupils (email/Learning Platform) should be on a professional level and only carried out using official school systems
- eSafety issues are embedded in all aspects of the curriculum and other school activities
- students/pupils understand and follow the school eSafety and acceptable use policy
- students/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 eSafety 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

- The ***Prevent*** message is adhered to when considering internet usage. All staff are expected to familiarise themselves with these issues first by familiarising themselves with the school's safeguarding policy and the document 'Keeping Children Safe in Education'. *https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/418686/Keeping_children_safe_in_education.pdf* Should they have any concerns regarding issues pertinent to the prevent agenda or indeed wider safeguarding issues, they should follow the process outlined for raising issues in the school's policy.

DSL/Child Protection Officer;
should be trained in eSafety 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

Safeguarding (eSafety) Committee;
Members of the safeguarding committee will assist the eSafety Coordinator with:

- the production/review/monitoring of the school eSafety policy/documents.
- the production/review/monitoring of the school filtering policy

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. (at KS1 it would be expected that parents/carers would sign on behalf of the pupils)
- 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 eSafety practice when using digital technologies out of school and realise that the school's eSafety 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 eSafety campaigns/literature. Parents and carers will be responsible for:

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

Community Users;

Community Users who access school ICT systems/website/Learning Platform as part of the Extended School provision will be expected to sign a Community User AUP before being provided with access to school systems.

Policy Statements

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 eSafety is therefore an essential part of the school's eSafety provision. Children and young people need the help and support of the school to recognise and avoid eSafety risks and build their resilience. eSafety education will be provided in the following ways:

- A planned eSafety programme should be provided as part of ICT/PHSE/other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school
- Key eSafety messages should be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities
- Students/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
- Pupils should be helped to understand the need for the pupil AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Rules for use of ICT systems/internet will be posted in all rooms
- Staff should act as good role models in their use of ICT, the internet and mobile devices

Parents/carers;

Many parents and carers have only a limited understanding of eSafety 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 and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide". (Byron Report).

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

- Letters, newsletters, web site, digital signage
- Parents' evenings

Extended Schools;

The school will offer family learning courses in ICT, media literacy and eSafety so that parents and children can together gain a better understanding of these issues. Messages to the public around e safety should also be targeted towards grandparents and other relatives as well as parents. Everyone has a role to play in empowering children to stay safe while they enjoy these new technologies, just as it is everyone's responsibility to keep children safe in the non-digital world.

Education & Training

Staff;

It is essential that all staff receive eSafety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal eSafety training will be made available to staff. An audit of the eSafety training needs of all staff will be carried out regularly.
- All new staff should receive eSafety training as part of their induction programme, ensuring that they fully understand the school eSafety policy and Acceptable Use Policies
- The eSafety Coordinator will receive regular updates through attendance at LA/other information/training sessions and by reviewing guidance documents released by BECTA/WBC and others.
- This eSafety policy and its updates will be presented to and discussed by staff in staff/team meetings/INSET days.
- The eSafety Coordinator will provide advice/guidance/training as required to individuals as required

Govemors;

Governors should take part in eSafety training/awareness sessions, with particular importance for those who are members of any committee/group involved in ICT/eSafety/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/equipment, filtering and monitoring;

The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their eSafety responsibilities:

School ICT systems will be managed in ways that ensure that the school meets the eSafety technical requirements outlined by Becta and the Acceptable Usage Policy

- School ICT systems must be regularly updated to ensure up-to-date anti-virus definitions and Microsoft Windows Security Updates are installed. Essential software i.e. Acrobat Reader, Flash Player, Java, Internet Explorer, Smartboard etc. must be kept current.
- 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
- All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the Network Manager and Business Manger and will be reviewed, at least annually, by the Safeguarding Committee
- All users will be provided with a username and password to access the school network by (Esafety co-ordinator and Business manager who will keep an up to date record of users and their usernames. Users will be required to change their password every term.

- The “master/administrator” passwords for the school ICT system, used by the Network Manager and Business Manager must also be available to the Head teacher or other nominated senior leader and kept in a secure place (eg school safe)
- School Data should be securely managed when taken off the school site using encrypted memory devices or password protected files.
- Users will be made responsible for the security of their username and password, 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.
- The school maintains and supports the managed filtering service provided by Warrington Borough Council.
- In the event of the Network Manager (or other person) needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Head teacher (or other nominated senior leader).
- Any filtering issues should be reported immediately to Warrington’s IT support on 2200.
- Requests from staff for sites to be added or removed from the filtered list will be considered at the appropriate senior level. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the eSafety Governor
- School ICT technical staff regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Policy.
- Remote management tools are used by staff to control workstations and view users activity
- An appropriate system is in place for users to report any actual/potential eSafety incident to the designated eSafety Co-ordinator (or other relevant person).
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.
- An agreed system is in place for the provision of temporary access of “guests” (eg trainee teachers, visitors) onto the school system.
- Staff/students/pupils/community users are able to use equipment for personal usage while they do not infringe AUP agreements and are inline with school policies. Their family members are allowed on laptops and other portable devices that may be used out of school.
- Staff are allowed to install programmes on school workstations/portable devices in accordance with AUP agreements and School policies.
- All removable media (e.g. memory sticks/CDs/DVDs) are allowed by users on school workstations/portable devices in accordance with AUP agreements and school policies.

Curriculum;
ESafety should be a focus in all areas of the curriculum and staff should reinforce eSafety messages in the use of ICT across the curriculum.

- eSafety should be taught regularly through a scheme of work with identified progression of knowledge, skills and understanding.
- eSafety 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, eg using search engines, staff should be vigilant in monitoring the content of the websites visited.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that they can temporarily be removed from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.
- 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
- 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 and video images - Photographic, Video;

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students/pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and students/pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate students/pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.
- Staff members are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should **not** be used for such purposes.
- Care should be taken when taking digital/video images that students/pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students/pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website (may be covered as part of the AUP signed by parents or carers at the start of the year
- Pupil's work can only be published with the permission of the pupil and parents or carers.

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, in line with school policy (below) once it has been transferred or its use is complete

Communications;

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks/disadvantages:

	Staff & other adults			Pupils			
Communication Technologies (outside of those available on the learning platform)	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	√					√		
Use of mobile phones in lessons							√	
Use of mobile phones in social time		√						√
Taking photos on mobile phones or other camera devices		√					√	
Use of hand held devices eg netbooks, PDAs, PSPs, iPad, iPod	√				√			
Use of personal email addresses in school, or on school network		√						√
Use of school email for personal emails		√						√
Use of chat rooms/facilities		√					√	
Use of instant messaging		√					√	

Use of social networking sites		√					√	
Use of blogs		√					√	

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

- Where available the official school email service may be regarded as safe and secure and is monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (eg by remote access).
- Users need to be aware that email communications may be monitored
- 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**.** These 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 these 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.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Unsuitable/inappropriate activities;

The school believes that the activities referred to in the following section would be inappropriate in a school context and 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:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
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:	**child sexual abuse images**				✓	✓
	promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation				✓	✓
	adult material that potentially breaches the Obscene Publications Act in the UK				✓	✓
	criminally racist material in UK				✓	✓
	pornography				✓	
	promotion of any kind of discrimination				✓	
	promotion of racial or religious hatred				✓	
	threatening behaviour, including promotion of physical violence or mental harm				✓	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				✓	
Using school systems to run a private business					✓	
Use systems, applications, websites or other mechanisms that bypass the filtering or other					✓	

safeguards employed by WBC and/or the school					
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions				✓	
Revealing or publicising confidential or proprietary information (eg financial/personal information, databases, computer/network access codes and passwords)				✓	
Creating or propagating computer viruses or other harmful files				✓	
Carrying out sustained or instantaneous high volume network traffic (downloading/uploading files) that causes network congestion and hinders others in their use of the internet				✓	
Online gaming (educational)					
Online gaming (non educational)					
Online gambling				√	
Online shopping/commerce					
File sharing					
Use of social networking sites					
Use of video broadcasting eg YouTube					

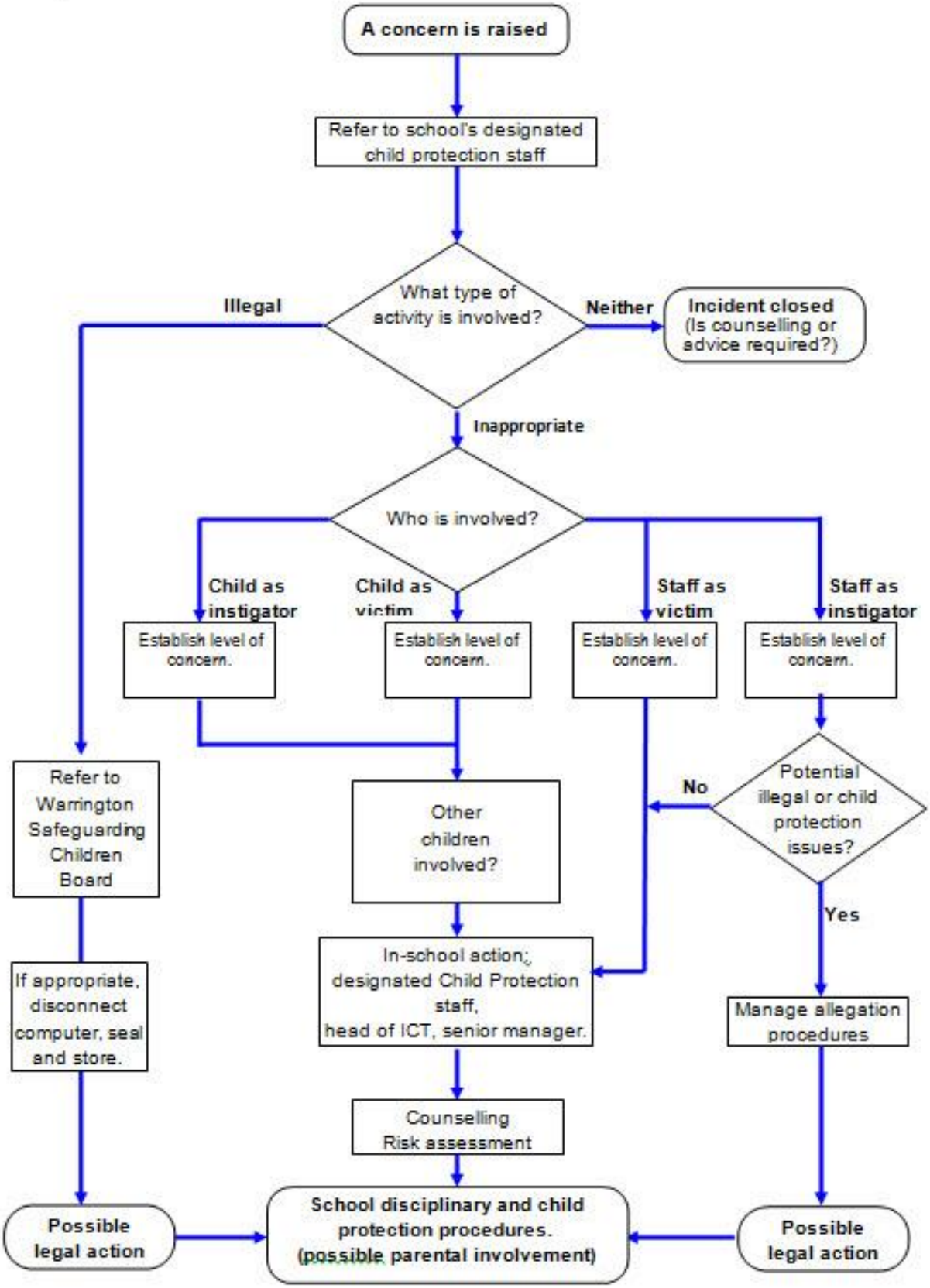
Responding to incidents of misuse;

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

The WBC flow chart – below and 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.

Response to an incident of concern



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 recommended that more than one member of staff is involved in the investigation which should be carried out on a "clean" designated computer.

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

Students/Pupils **Actions/Sanctions**

Incidents:	Refer to class teacher	Refer to Head of Department	Refer to Head teacher	Refer to Police	Refer to technical support staff for action re filtering/security etc	Inform parents /carers	Removal of network/ internet access rights	Warning	Further sanction eg detention/exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities).	√							√	
Unauthorised use of non-educational sites during lessons	√							√	
Unauthorised use of mobile phone/digital camera/other handheld device									
Unauthorised use of social networking/instant messaging/personal email	√				√	√		√	
Unauthorised downloading or uploading of files									
Allowing others to access school network by sharing username and passwords	√				√	√		√	
Attempting to access or accessing the school network, using another student's/pupil's account	√				√	√		√	
Attempting to access or	√				√			√	√

accessing the school network, using the account of a member of staff									
Corrupting or destroying the data of other users	√	√					√	√	√
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	√		√	√		√		√	√
Continued infringements of the above, following previous warnings or sanctions		√				√	√		√
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school			√	√					√
Using proxy sites or other means to subvert the school's filtering system			√			√		√	√
Accidentally accessing offensive or pornographic material and failing to report the incident			√		√			√	
Deliberately accessing or trying to access offensive or pornographic material			√	√					√
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act			√						√

Staff **Actions / Sanctions**

Incidents:	Refer to line manager	Refer to Head teacher	Refer to Local Authority/ HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities).	√	√	√			√		
Excessive or inappropriate personal use of the internet/social networking sites/instant messaging/personal email	√	√				√		
Unauthorised downloading or uploading of files	√	√				√		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	√	√						
Careless use of personal data eg holding or transferring data in an insecure manner	√	√	√					√
Deliberate actions to breach data protection or network security rules	√	√	√					√
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	√	√	√					√
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	√	√	√					√
Using personal email/social networking/instant messaging/text messaging to carrying out digital communications with students/pupils	√	√	√					√
Actions which could compromise the staff member's professional standing	√	√	√					√
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	√	√	√					√
Using proxy sites or other means to subvert the school's filtering system	√	√	√					√
Accidentally accessing offensive or pornographic material and failing to report	√	√				√		

the incident								
Deliberately accessing or trying to access offensive or pornographic material	√	√	√	√				√
Breaching copyright or licensing regulations	√	√	√			√		
Continued infringements of the above, following previous warnings or sanctions	√	√	√					√

Appendices;

- eSafety Framework for schools
- Student/Pupil Acceptable Usage Policy
- Staff and Volunteers Acceptable Usage Policy
- Parents /Carers Acceptable Usage Policy Agreement
- School Filtering Policy
- School Password Security Policy
- School Personal Data Policy
- School eSafety Charter
- Legislation
- Glossary of terms

ESafety Framework;

Initial	Developmental	Established	Advanced
Acceptable Use Policy There is an Acceptable Use Policy which is used for reference	There is an Acceptable Use Policy which is used for reference and shared with and signed by parents/guardians. All users have been informed of their responsibilities outlined in the schools AUP The AUP is not rigorously followed by learners.	The Acceptable Use Policy has been developed by the school through its stakeholders. The AUP is signed by all users of the learning network and visible to all. The AUP is followed by most learners and implemented by staff.	The Acceptable Use Policy has been developed by all stakeholders in the school and is referred to regularly and updated. The AUP is signed and has been adopted by all users of the learning network and implemented by all learners and staff and is visible to all. The AUP is reviewed at least annually.
Designated member of staff There is a designated member of staff who is responsible for eSafety developments in school.	There is a designated member of staff, an eSafety officer, who is up-to-date with local and national initiatives.	There is an identified eSafety officer who is responsible for eSafety developments in school and sharing of practice with staff.	There is an identified eSafety officer who is responsible for eSafety developments in school and sharing of practice with staff and the wider community.
Monitoring Monitoring of inappropriate use of technology is not carried out	Monitoring of inappropriate use of technology is done on an ad hoc basis using school staff and expertise.	Schools have adopted robust and sustainable monitoring systems, monitoring on a regular basis to support productive collaboration and personalisation strategies. Network and internet access monitoring is done by an assigned person using monitoring software and issues acted upon.	All recognise their commitment to their community and each other in keeping all safe to pursue productive gains in the use of collaborative technology. Monitoring is done on a regular basis by an assigned person using monitoring software and issues are referred to appropriate personnel.
Data security		There is a mandatory level of information security required in all schools. The school is aware of and implementing the guidance. Refer to Becta for guidance	
School improvement planning There is no evidence of integration of eSafety with other areas of the school	There is little evidence of integration of eSafety with other areas of the school improvement plan.	There is evidence of integration of eSafety with other areas of the school improvement plan.	ESafety is fully integrated with other areas of the school improvement plan.

Initial	Developmental	Established	Advanced
improvement plan.			
Teaching and curriculum Some pupils receive eSafety teaching as part of their curriculum	Most pupils receive eSafety teaching as part of their curriculum. ESafety is discussed in an informal and ad hoc manner. There is little curriculum support and only within the ICT curriculum.	Most users receive eSafety teaching as part of their curriculum /professional development. Teachers are referring to eSafety in planning and teaching. ESafety is embedded within the curriculum for all year groups and appropriate resources are used to support learning.	All users regularly receive eSafety teaching as part of their curriculum /professional development. Teachers are referring to eSafety in planning and teaching. ESafety is embedded within the curriculum for all year groups and appropriate resources are used to support learning. ESafety is seen as an evolving dialogue.
ESafety resources eSafety resources are used on an ad hoc basis to support teachers' understanding	ESafety resources are used by some teachers to support their understanding and there are opportunities to use a wide range of resources and the internet.	Appropriate eSafety resources are used by most teachers to support their understanding and there are opportunities to use a wide range of resources and the internet.	Appropriate eSafety resources are used by all teachers to support their understanding and there are opportunities to use a wide range of resources and the internet.

Pupil Acceptable Use Policy Agreement

School Policy

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. Young people should have an entitlement to safe internet access at all times.

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 *students/pupils* will have good access to ICT to enhance their learning and will, in return, expect the *students/pupils* to agree to be responsible users.

Pupil 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.

For my own personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I will not share my password, nor will I try to use any other person's username and password.
- I will be aware of "stranger danger", when I am communicating online.
- I will not disclose or share personal information about myself or others when online.
- If I arrange to meet people that I have only communicated with online, I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it online.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the school ICT systems are primarily intended for educational use and that I will not use the systems for personal or recreational use unless I have permission to do so.
- 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 use the school ICT systems for online gaming, online gambling, internet shopping, file sharing, or video broadcasting (eg YouTube), unless I have permission of a member of staff to do so.
- I will act as I expect others to act toward me:
- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

- I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:
- I will only use my personal hand held/external devices (mobile phones/USB devices etc) in school if I have permission .I understand that, if I do use my own 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 understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I 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 immediately report any damage or faults involving equipment or software, however this may have happened.

- I will not open any attachments to emails, unless I know and trust the person/organisation who sent the email, due to the risk of the attachment containing viruses or other harmful programmes.
- 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 only use chat and social networking sites with permission and at the times that are allowed When using the internet for research or recreation, I recognise that:

- I should 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 try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the school network/internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school ICT systems.

Pupil Acceptable Use Agreement Form

This form relates to the pupil Acceptable Use Policy (AUP), to which it is attached.
Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school ICT systems.

I have read and understand the above and agree to follow these guidelines when:

- I use the school ICT systems and equipment (both in and out of school)
- I use my own equipment in school (when allowed) eg mobile phones, PDAs, cameras etc
- I use my own equipment out of school in a way that is related to me being a member of this school eg communicating with other members of the school, accessing school email, learning platform, website etc.

Name of Student/Pupil

Group/Class

Signed Date

Staff (and Volunteer) Acceptable Use Policy Agreement Template;

School Policy

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. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers 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.
- that staff are protected from potential risk in their use of ICT in their everyday work.

The school will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for *pupils* learning and will, in return, expect staff and volunteers to agree to be responsible users.

Staff 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 students/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 eSafety in my work with young people.

For my professional and personal safety:

- 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 immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school ICT systems:

- 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. Where these images are published (eg on the school website/learning platform) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use chat and social networking sites in school in accordance with the school's policies.
- I will only communicate with students/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.

- The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:
- When I use my personal hand held/external devices (PDAs/laptops/mobile phones/USB devices etc) 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 use personal email addresses on the school ICT systems inline with the schools agreed policies.
- 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, in accordance with relevant school policies.
- 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, unless this is allowed in school policies.
- 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/LA Personal Data 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 student/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 immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- 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 Acceptable Use Policy Agreement;

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. Young people should have an entitlement to safe internet access at all times.

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.
- that parents and carers are aware of the importance of eSafety and are involved in the education and guidance of young people with regard to their online behaviour.

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. A copy of the Pupil Acceptable Use Policy is attached to this permission form, so that parents/carers will be aware of the school expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

Permission Form

Parent/Carers Name

Student/Pupil Name

As the parent/carer of the above Pupils, 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, eSafety 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 eSafety.

Signed Date

School Filtering Policy

Rationale

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.

Purpose

To;

- provide within reason appropriate safety procedures that support the safe guard pupils against any illegal and inappropriate materials that they may come into contact with
- ensure appropriate filters are in place and are being effective
- ensure when filter if breached it is logged and monitored
- to monitor the effectiveness of the filter and supporting processes

Responsibilities

The responsibility for the management of the school's filtering policy will be held by a network Manager. 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 (Designated child protection person):
- be reported to and authorised by a second responsible person prior to changes being made
- be reported to the Safe Guarding Committee in the form of an audit of the change control logs

All users have a responsibility to report immediately to eSafety co-ordinator 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 eSafety 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 and through eSafety awareness sessions/newsletter etc.

Changes to the Filtering System

- Staff who wish to request changes to the filtering will only be allowed if they can demonstrate that it is to the educational benefit of the child and or activity that pupils are currently engaged in.
- The school will allow access to social networking sites (or other specific sites identified) for some users for limited periods of times under the supervision of staff. Staff should be able to demonstrate be strong educational reasons for such agreed changes).
- Designated Child Protection officer will be the second responsible person involved in providing checks and balances (preferably this will be at the time of request, but could be retrospectively through inspection of records / audit of logs)
- Net work Manager/ eSafety co-ordinator will keep detailed loggs of random sampling of handheld devises, breaches in the filtering system and incidents of eSafety infringements that will be termly presented to Safe Guarding committee.

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 eSafety co-ordinator who will decide whether to make school level changes. If it is felt that the site should be filtered (or unfiltered) at Warrington level, the responsible person eSafety co-ordinator should contact the ICT Help Desk with the URL.

Monitoring

No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network and on school equipment as indicated in the School eSafety Policy and the Acceptable Use agreement. Monitoring will take place as follows:

- Random sampling of handheld devises and work stations
- Specialist software programme checks (to be purchased)

Audit/Reporting

Logs of filtering change controls and of filtering incidents will be made available to:

- the second responsible person designated child protection officer
- Safeguarding Committee
- Local Authority on request

The filtering policy will be reviewed in the response to the evidence provided by the audit logs of the suitability of the current provision.

School Password Security Policy

Rationale

The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible. A safe and secure username/password system is essential if the above is to be established and will apply to all school ICT systems, including email and Learning Platform.

Purpose;

- users can only access data to which they have right of access

- no user should be able to access another's files, without permission (or as allowed for monitoring purposes within the school's policies).
- 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

Broad Guidelines

The management of the password security policy will be the responsibility of Network Manager and Business Manger

All users (adults and young people) will have responsibility for the security of their username and password, 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. With exception of a class log in

Passwords for new users, and replacement passwords for existing users can be allocated by network manager. Any changes carried out must be notified to the manager of the password security policy.

Users will change their passwords every Term

Training/Awareness

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

- at induction
- through the school's eSafety 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 eSafety lessons
- through the Acceptable Use Agreement

Policy Statements

All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the Network Manager (or other person) and will be reviewed, at least annually, by the eSafety Committee (or other group).

All users will be provided with a username and password by network manager who will keep an up to date record of users and their usernames. Users will be required to change their password every term.

The administrator passwords for the school ICT system, used by the Network Manager must also be available to the Head teacher or other nominated senior leader and kept in a secure place (eg school safe). Alternatively, where the system allows more than one master/administrator log-on, the Head teacher or other nominated senior leader should be allocated those master/administrator rights. A school should never allow one user to have sole administrator access.

Audit/Monitoring/Reporting/Review

The responsible person will ensure that full records are kept of:

- User Ids and requests for password changes
- User log-ons
- Security incidents related to this policy

In the event of a serious security incident, the police may request and will be allowed access to passwords used for encryption.

Local Authority Auditors also have the right of access for audit investigation purposes

User lists, IDs and other security related information must be given the highest security classification and stored in a secure manner.

These records will be reviewed by ... *(eSafety co-ordinator, Safeguarding Committee* at regular intervals per term.

This policy will be regularly reviewed annually in response to changes in guidance and evidence gained from the logs.

School Personal Data Handling Policy

Rationale

Schools should do everything within their power to ensure the safety and security of any material of a personal or sensitive nature (Becta – Good Practice in information handling in schools – keeping data secure, safe and legal – Sept 2008).

It is the responsibility of all members of the school community to take care when handling, using or transferring personal data that it can not 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.

Anyone who has access to personal data must know, understand and adhere to this policy, which brings together the legal requirements contained in relevant data legislation and relevant regulations and guidance from the Local Authority.

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”.

Purpose

To;

- Ensure the integrity and safety of personal data from any unauthorised access
- To state clearly the schools position and procedures on personal data management
- To safeguard personal data from all those who do not have a need and permission to access it

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. (schools are responsible for their own registration)

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 pupils/students of the data they hold on the pupils/students, the purposes for which the data is held and the third parties (eg LA, DCSF, QCA, Connexions etc) to whom it may be passed. This fair processing notice will be passed to parents/carers through, Prospectus, a specific letter and newsletters .Parents/carers of young people who are new to the school will be provided with the fair processing notice through the school prospectus.

A copy of a specimen fair processing notice can be found at:
http://www.teachernet.gov.uk/management/ims/datamanagement/fpnpupils/. It contains a relevant wording for the regulations pertaining to the transfer of information to Connexions, in secondary schools and new requirements resulting from the introduction of Contact Point. A new specimen FPN is available for 2008/9. Schools are advised to contact their Local Authority for local versions of the Fair Processing Notice.

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
- Day to day support and guidance from Information Asset owners

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.

All users will be given secure user names and strong passwords which must be changed regularly User names and passwords must never be shared.

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 (i.e. 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. (the school will need to set its own policy, relevant to its physical layout, type of ICT systems etc)

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 pupil working from their home 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. (nb. to carry encrypted material is illegal in some countries)

(Schools will find detailed guidance on data encryption in the Becta document “Good practice in information handling in schools – Data Encryption - a guide for staff and contractors tasked with implementing a system of secure data encryption and deletion”)

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 (see further reading section for reference to the Cabinet Office guidance), and other media must be shredded, incinerated or otherwise disintegrated for data.

A Destruction Log should be kept of all data that is disposed of. The log should include the document ID, classification, date of destruction, method and authorisation.

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 responsible individuals. Business Manager

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 at evidential quality for seven years.

(Schools will find detailed guidance on audit logging in the Becta document "Good practice in information handling in schools - audit logging and incident handling - a guide for staff and contractors tasked with implementing data security")

The school has a policy for reporting, managing and recovering from information risk incidents, which establishes: (schools should determine their own reporting policy, in line with that of their LA, and add details here)

- 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.

Further reading

Teachernet – Data processing and sharing -
http://www.teachernet.gov.uk/management/atoz/d/dataprocessing/

Office of the Information Commissioner website:
http://www.informationcommissioner.gov.uk

Office of the Information Commissioner – guidance notes: Access to pupil's information held by schools in England

Becta – Good Practice in information handling in schools – keeping data secure, safe and legal and it's four detailed appendices: (September 2008)

http://schools.becta.org.uk/upload-dir/downloads/information_handling.pdf
http://schools.becta.org.uk/upload-dir/downloads/information_handling_impact_levels.pdf
http://schools.becta.org.uk/upload-dir/downloads/data_encryption.pdf
http://schools.becta.org.uk/upload-dir/downloads/audit_logging.pdf
http://schools.becta.org.uk/upload-dir/downloads/remote_access.pdf

Cabinet Office – Data handing procedures in Government – a final report (June 2008)
http://www.cabinetoffice.gov.uk/reports/data_handling.aspx

Name of School	
Name of Local Authority	

We are working with staff, pupils and parents/carers to create a school community which values the use of new technologies in enhancing learning, encourages responsible use of ICT, and follows agreed policies to minimise potential eSafety risks.

Our school community

Discusses, monitors and reviews our eSafety **policy** on a regular basis. Good practice suggests the policy should be reviewed annually or at most every two years.

Supports **staff** in the use of ICT as an essential tool for enhancing learning and in the embedding of eSafety across the whole school curriculum.

Ensures that **pupils** are aware, through eSafety education, of the potential eSafety risks associated with the use of ICT and mobile technologies, that all eSafety concerns will be dealt with sensitively and effectively; that pupils feel able and safe to report incidents; and that pupils abide by the school's eSafety policy.

Provides opportunities for **parents/carers** to receive eSafety education and information, to enable them to support their children in developing good eSafety behaviour. The school will report back to parents / carers regarding eSafety concerns. Parents/carers in turn work with the school to uphold the eSafety policy.

Seeks to learn from eSafety good practice elsewhere and utilises the support of the **LA, NWGfL and relevant organisations** when appropriate.

Chair of Governors	
Head teacher	
Pupil Representative	

Legislation;

Legislative framework under which this eSafety Policy and guidance has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

It is recommended that legal advice is sought in the advent of an e safety issue or situation.

Computer Misuse Act 1990;

This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- "Eavesdrop" on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

Data Protection Act 1998;

This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept longer than necessary.
- Processed in accordance with the data subject's rights.
- Secure.
- Not transferred to other countries without adequate protection.

Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications Act 2003

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000
It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
- Ascertain whether the communication is business or personal;
- Protect or support help line staff.
- The school reserves the right to monitor its systems and communications in line with its rights under this act.

Trade Marks Act 1994
This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, Designs and Patents Act 1988
It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. YouTube).

Telecommunications Act 1984
It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994
This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they: -

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Racial and Religious Hatred Act 2006
This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Protection of Children Act 1978
It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison

Sexual Offences Act 2003
The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986
This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence. Children, Families and Education Directorate page 38 April 2007.

Obscene Publications Act 1959 and 1964;
Publishing an “obscene” article is a criminal offence. Publishing includes electronic transmission.

Human Rights Act 1998
This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of “higher law”, affecting all other laws. In the school context, human rights to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

The Education and Inspections Act 2006;
Empowers Head teachers, to such extent as is reasonable, to regulate the behaviour of students/pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

Glossary of terms

AUP Acceptable Use Policy – see templates earlier in this document

Becta British Educational Communications and Technology Agency (Government agency promoting the use of information and communications technology)

CEOP Child Exploitation and Online Protection Centre (part of UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes.

CPD Continuous Professional Development

CYPS Children and Young Peoples Services (in Local Authorities)

DCSF Department for Children, Schools and Families

ECM Every Child Matters

FOSI Family Online Safety Institute

HSTF Home Secretary's Task Force on Child Protection on the Internet

ICO Information Commissioners Office

ICT Information and Communications Technology

ICTMark Quality standard for schools provided by Becta

INSET In Service Education and Training

IP address The label that identifies each computer to other computers using the IP (internet protocol)

ISP Internet Service Provider

ISPA Internet Service Providers' AssociationStree

IWF Internet Watch Foundation

JANET Provides the broadband backbone structure for Higher Education and for the National Education Network and RBCs.

KS1 Key Stage 1 (2, 3, 4 or 5) – schools are structured within these multiple age groups eg KS3 = years 7 to 9 (age 11 to 14)

LA Local Authority

LAN Local Area Network

Learning A learning platform brings together hardware, software and supporting services

Platform to support teaching, learning, management and administration.

LSCB Local Safeguarding Children Board

MIS Management Information System

MLE Managed Learning Environment

NEN National Education Network – works with the Regional Broadband Consortia (eg NWGfL) to provide the safe broadband provision to schools across Britain.

Ofcom Office of Communications (Independent communications sector regulator)

Ofsted Office for Standards in Education, Children's Services and Skills

PDA Personal Digital Assistant (handheld device)

PHSE Personal, Health and Social Education

RBC Regional Broadband Consortia (eg SWGfL) have been established to procure broadband connectivity for schools in England. There are 10 RBCs covering 139 of the 150 local authorities:

SEF Self Evaluation Form – used by schools for self evaluation and reviewed by Ofsted prior to visiting schools for an inspection

SRF Self Review Form – a tool used by schools to evaluate the quality of their ICT provision and judge their readiness for submission for the ICTMark

NWGfL North West Grid for Learning – the Regional Broadband Consortium of NW Local Authorities – is the provider of broadband and other services for schools and other organisations in the NW

TUK Think U Know – educational eSafety programmes for schools, young people and parents.

VLE Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting,

WAP Wireless Application Protocol