St Werburgh's Catholic Primary School
E Safety Policy

Background

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 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 and young people should have an entitlement to safe internet access at all times. The requirement to ensure that children and young people 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.

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 Digital Safety policy is used in conjunction with other school policies (e.g., behaviour, child protection and safeguarding 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.

The school 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 Digital 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.

Development of this Policy

This Digital Safety policy has been developed through discussion/involvement with the following people. It should be read in conjunction with all Safeguarding Policies.

- *Headteacher/Designated Safeguarding Lead*
- *Safeguarding Governor*
- *Computing Subject Leaders*
- *Teachers*
- *Teaching Assistants*
- *Governors*
- *Local Authority*

Scope of the Policy

This policy applies to all members of the school community (including staff, pupils, volunteers, parents / carers, visitors who have access to and are users of school ICT systems
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 Digital 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 policy and will, where known, inform parents / carers of incidents of inappropriate Digital Safety behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the roles and responsibilities for Digital Safety of individuals and groups within St Werburgh's Catholic Primary School:

Governors:

Governors are responsible for the approval of the Digital Safety Policy and for reviewing the effectiveness of the policy. Our Governors, Liz Hawkins and Giuseppe Roberto have been appointed as Lead Governor for safeguarding which includes all aspects of E Safety. Any incidents will be reported to the full Governing Body.

Headteacher/Designated Lead for Safeguarding

- The Headteacher is responsible for ensuring the safety (including Digital Safety) of members of St Werburgh's Catholic Primary School community.
- receives reports of Digital Safety incidents and creates a log of incidents to inform future Digital Safety developments
- meets regularly with Safeguarding Governor to discuss current issues, review incident logs and filtering / change control logs in consultation with Computing Lead.
- The Headteacher will ensure that there are procedures to follow in the event of a serious E safety allegation

- The Headteacher is the designated lead for child protection and is trained in Digital Safety issues and should be aware of the potential for serious child protection issues to arise from:
    - sharing of personal data
    - access to illegal / inappropriate materials or inappropriate on-line contact with adults / strangers o potential or actual incidents of grooming
    - cyber-bullying

  (N.B. it is important to emphasise that these are child protection issues, not technical issues, simply which the technology provides additional means for child protection issues to develop.)

Computing Coordinator (liaising with Headteacher)

- takes day to day responsibility for Digital Safety issues
- ensures that all staff are aware of the procedures that need to be followed in the event of a Digital Safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority and Technicians (Wirral LA)
- reports regularly to Senior Leadership Team

Technical Support staff:

The school's hi-impact IT Technician is responsible for ensuring:

- that the St Werburgh's Catholic Primary School's ICT infrastructure is secure and is not open to misuse or malicious attack
- that the school meets the Digital Safety technical requirements outlined in relevant Local Authority Digital Safety Policy and guidance
- that users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed
- 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 he/she keeps up to date with Digital Safety technical information in order to effectively carry out their Digital Safety role and to inform and update others as relevant
- that the use of the network / remote access is regularly monitored in order that any misuse / attempted misuse can be reported to the Digital Safety lead 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 Digital Safety matters and of the current school Digital 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 ICT Co-ordinator /Headteacher for investigation
- digital communications with pupils (email /Virtual Learning Environment (VLE) should be on a professional level and only carried out using official school systems
- Digital Safety issues are embedded in all aspects of the curriculum and other school activities
- pupils understand and follow the school Digital Safety and acceptable use policy
- they monitor ICT activity in lessons, extra-curricular and extended school activities
- they are aware of Digital Safety issues related to the use of mobile phones, cameras and handheld 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

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.
- 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 handheld 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 Digital Safety practice when using digital technologies out of school and realise that the school's Digital 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 newsletters, letters, website and information about national / local Digital Safety campaigns / literature. Parents and carers will be responsible for:

- endorsing the Pupil Acceptable Use Policy
- accessing the St Werburgh's Catholic Primary School website in accordance with the relevant school Acceptable Use Policy.

Policy Statements Education and Curriculum - 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 Digital Safety is therefore an essential part of the school's Digital Safety provision. Children and young people need the help and support of the school to recognise and avoid Digital Safety risks and build their resilience.

Digital Safety education will be provided in the following ways:

- A planned Digital Safety programme will be provided as part of Computing/ PSHE / other lessons and will be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school
- Key Digital Safety messages should be reinforced as part of a planned programme of assemblies
- Pupils will be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information
- Pupils will 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
- Rules for use of ICT/internet will be on display in all rooms to remind children
- Staff should act as good role models in their use of ICT, the internet and mobile devices

Curriculum

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

- 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 the young people visit.
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line 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.

Education – parents / carers

Many parents and carers have only a limited understanding of Digital Safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line 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, website,
- Parents meetings

St Werburgh's Catholic Primary School will sign post families to local family learning courses in ICT, media literacy and Digital Safety 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 nondigital world.

Education & Training – Staff

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

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

Training – Governors

Governors should take part in Digital Safety training / awareness sessions, with particular importance for those who are members of ICT working party / group involved in ICT / Digital 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
- Updates by visiting speakers at Full Governing Body Meetings

Technical – infrastructure / equipment, filtering and monitoring

St Werburgh's Catholic Primary School will be responsible for ensuring that the school 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 Digital Safety responsibilities:

- School ICT systems will be managed in ways that ensure that the school meets the Digital Safety technical requirements outlined in the Acceptable Usage Policy and any relevant Local Authority Digital Safety Policy and guidance
- 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.
- All users will be provided with a username and password Users will be required to change their password every year.
- The "master / administrator" passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the Headteacher or other nominated senior leader and kept in a secure place (e.g., school safe)
- 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 Wirral IT
- 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 Headteacher (or other nominated senior leader).
- Any filtering issues should be reported immediately to the E safety Co-ordinator
- Requests from staff for sites to be removed from the filtered list will be considered by the E safety co-ordinator and Headteacher, and if the request is agreed, this action will be recorded, and logs of such actions shall be reviewed regularly by the Digital Safety Working party
- School ICT technical staff regularly monitor and record the activity of users on the school ICT systems
- The school infrastructure and individual workstations are protected by up-to-date virus software.

Education / Training / Awareness

Pupils will be made aware of the importance of filtering systems through the Digital 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: (amend as relevant)

- *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 Digital Safety awareness sessions / newsletter etc.

Use of digital and video images - Photographic, Video

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. However, staff and 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. St Werburgh's Catholic Primary 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 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 e.g., 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, or on equipment specifically designated for school use.
- 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
- 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.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Permission of parents is sought for pupils and their work to be shared via the school Twitter account

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018 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.

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 and volunteers				Pupils		
Communication technologies	Allowed	Allowed at certain times	Allowed for designated staff	Not allowed	Allowed	Allowed at certain times	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				✓			✓
Taking photos on designated ipads for school use	✓					✓	
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 with the exception of our school twitter account.		✓					✓

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

- The official school email service may be regarded as safe and secure
- 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 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

Some internet activity e.g., accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other ICT systems. Other activities e.g., Cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

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

User Actions:

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, e.g., 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

The above actions are unacceptable and where illegal activity takes place, it will be reported to the police.

Other prohibited activity:

- Using school systems to run a private business

- Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards
- 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 (e.g., 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

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

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. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:
At St Werburgh's Catholic Primary School E Safety incidents are logged on CPOMS.

Incidents:Pupils	Refer to class teacher	Refer to Headteacher	Refer to police	Refer to hi-impact for action re filtering/security	Inform parent/Carer	Removal of access rights	Warning
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		✓			✓		✓
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		✓	✓	✓	✓	✓	✓

Incidents:Staff	Refer to Headteacher	Refer to LADO/HR	Refer to police	Refer to hi-impact for action re filtering	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 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	✓	✓		✓	✓	✓	✓
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

- Acceptable Use Policy Agreement - F1, F2, Year 1 and 2
- Acceptable Use Policy Agreement -Year 3 and 4
- Acceptable Use Policy Agreement - Year 5 and 6
- Acceptable Use Policy Agreement – Staff and Volunteers
- Acceptable Use Policy Agreement – Parent/Carer
- Wirral - Use of Social Networking sites
- Camera Use Policy
- Camera and Video Courtesy Code
- E Safety Incidents Proforma
- School Password Security Policy
- Useful Websites
- Glossary of terms

(F1, F2, Yr1 & Yr2)
Acceptable Use Policy Agreement

I want to feel safe all the time.

I agree that I will:

- **Always keep my passwords a secret**
- **Only open pages which my teacher has said are OK**
- **Tell my teacher if anything makes me feel scared or uncomfortable**
- **Not give my mobile phone number to anyone who is not a friend in real life**
- **Talk to my teacher before using anything on the internet**
- **Not tell people about myself online (I will not tell them my name, anything about my home and family and pets)**

Anything I do on the computer may be seen by someone else

Name:		**Year group:**
Signed:		**Date:**

Years 3 and 4
Acceptable Use Policy Agreement

I want to feel safe all the time.

I agree that I will:

- **Always keep my passwords a secret**
- **Only open pages which my teacher has said are OK**
- **Only work with people I know in real life**
- **Tell my teacher if anything makes me feel scared or uncomfortable**
- **Make sure all messages I send are polite**
- **Show my teacher if I get a nasty message**
- **Not reply to any nasty message or anything which makes me feel uncomfortable**
- **Not give my mobile phone number to anyone who is not a friend in real life**
- **Talk to my teacher before using anything on the internet**
- **Not tell people about myself online (I will not tell them my name, anything about my home and family and pets)**
- **Not load photographs of myself onto a computer/ipad/phone**
- **Never agree to meet a stranger**

Anything I do on the computer may be seen by someone else

Name:		**Year group:**
Signed:		**Date:**

Years 5 and 6
Acceptable Use Policy Agreement

When I am using the computer or other technologies, I want to feel safe all the time. I agree that I will:

- **Always keep my passwords a secret**
- **Only visit sites which are appropriate to my work at the time**
- **Work in collaboration only with friends and I will deny access to others**
- **Tell a responsible adult straight away if anything makes me feel scared or uncomfortable**
- **Make sure all messages I send are respectful**
- **Show a responsible adult if I get a nasty message or get sent anything that makes me feel uncomfortable**
- **Not reply to any nasty message or anything which makes me feel uncomfortable**
- **Not give my mobile phone number to anyone who is not a friend**
- **Only e mail people I know or those approved by a responsible adult**
- **Talk to a responsible adult before joining chat rooms or networking sites**
- **Always keep my personal details private. (My name, family information, journey to school, my pets and hobbies etc)**
- **Always check with a responsible adult and my parents before I show photographs of myself**
- **Never meet an online friend without taking a responsible adult that I know with me**

I know that once I post a message or an item on the internet then it is completely out of my control.
I know that anything I write or say or any website that I visit may be being viewed by a responsible adult.

I agree that I will not:

Visit internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:

- **Inappropriate material**
- **Promoting discrimination of any kind**
- **Promoting illegal acts**
- **Break any school Digital Safety rule**
- **Do anything which exposes other children to danger**

I accept that my use of the school and Local Authority ICT facilities may be monitored, and the outcomes of the monitoring may be used.

Name:		**Year group:**
Signed:		**Date:**

ACCEPTABLE USE POLICY AND AGREEMENT

Introduction

This policy is designed to enable acceptable use for staff and governors.
St Werburgh's Catholic Primary School provides a range of ICT resources which are available to staff members and governors. In order to ensure the safety of both staff, governors and pupils, it is important that all staff members and governors follow the guidelines detailed below.
This policy aims to:

- Promote the professional, ethical, lawful and productive use of the School's ICT systems and infrastructure.
- Define and identify unacceptable use of the school's ICT systems and external systems.
- Educate users about their data security responsibilities.
- Describe why monitoring of the ICT systems may take place.
- Define and identify unacceptable use of social networking sites and school devices.
- Specify the consequences of non-compliance.

This policy applies to staff members and governors, and all users of the School's ICT systems are expected to read and understand this policy. To confirm acceptance of the policy, users will sign an Acceptable Use Agreement which is attached to this policy. Breach of this policy may result in disciplinary action.
The use by staff and monitoring by the school of its electronic communications systems is likely to involve the processing of personal data and is therefore regulated by the Data Protection Act 2018, together with the Employment Practices Data Protection Code issued by the Information Commissioner. Staff are referred to the School's Data Protection Policy for further information. If you are in doubt and require clarification on any part of this document, please speak to the IT Leader or Headteacher.

Provision of ICT Systems

All equipment that constitutes the School's ICT systems is the sole property of the school.
No personal equipment should be connected to or used with the School's ICT systems. Users must not try to install any software on the ICT systems without permission from the IT Leader or Headteacher. If software is installed without permission, it may cause extensive damage to the ICT systems and users could be held personally liable for any costs incurred in rectifying the damage.
The IT Leader is responsible for purchasing and/or allocating ICT equipment to individuals. Individual laptop/desktop computers or ICT equipment may be removed at any time, without prior warning, for regular maintenance, reallocation or any other operational reason. Maintenance includes, but is not limited to, new software installations, software updates, reconfiguration of settings and computer re-imaging.
Users are not permitted to make any physical alteration, either internally or externally, to the school's computer and network hardware.

Network access and security

All users of the ICT systems at the school must first be registered. Following registration, a network user account will be created, consisting of a username, password and an e-mail address. All passwords should be complex to ensure data and network security. All user account details are for the exclusive use of the individual to whom they are allocated. Staff are responsible for ensuring their password remains confidential and their account is secure. Passwords must be regularly changed.
All users are personally responsible and accountable for all activities carried out under their user account(s). Users must take all reasonable precautions to protect their user account details and must not share them to any other person, except to designated members of school staff for the purposes of system support. Users must report any security breach or suspected breach of their network, email or application account credentials to the IT Leader/HT as soon as possible.

Users should only access areas of the school's computer systems to which they have authorised access.
When any computer is left unattended, it must either be logged off or locked. Activity that threatens the integrity of the school ICT systems, or activity which attacks or corrupts other systems, is forbidden. Users' internet activity must not compromise the security of the data on the school ICT systems or cause difficulties for any other users.
Under no circumstances should a pupil be allowed to use a staff computer account.

School Email

Where email is provided, it is for academic and professional use. Wherever possible, all school related communication must be via the school email address.
The sending of emails is subject to the following rules:

- Language must not include swear words or be offensive or abusive.
- Emails or attachments of a pornographic, illegal, violent, sexist or racist nature are not permitted.
- Sending of attachments which contain copyright material to which the school does not have distribution rights is not permitted.
- The use of personal email addresses by staff for any official school business is not permitted.
- The forwarding of any chain messages/emails etc. is not permitted. Spam or junk mail will be blocked and reported to the email provider.
- Any electronic communication which contains any content which could be subject to data protection legislation (e.g., sensitive or personal information) will only be sent using secure and encrypted email or password protection.
- Emails should never contain children's full names either in the subject line or preferably not in the main body of the text. Initials should be used wherever possible.
- Access to school /setting email systems will always take place in accordance with data protection legislation and in line with other appropriate school/setting policies e.g., confidentiality.
- Members of the community must immediately tell a designated member of staff if they receive offensive communication, and this will be recorded in the relevant files/records (such as safeguarding).
- Staff will be encouraged to develop an appropriate work life balance when responding to email.
- Emails sent to external organisations should be written carefully and checked before sending, in the same way as a letter written on school headed paper would be.
- School email addresses and other official contact details will not be used for setting up personal social media accounts.

Internet Access

Internet access is provided for academic and professional use. Priority must always be given to academic and professional use.
The school's internet connection is filtered, meaning that a large amount of inappropriate material is not accessible. However, on occasions it may be possible to view a website which is inappropriate for use in a school. In this case the website must be reported immediately to the IT Leader and/or HT.
Staff must not therefore access from the school's system any web page or any files downloaded from the web which could be regarded as illegal, offensive, in bad taste or immoral.
Misuse of the internet may, in certain circumstances, constitute a criminal offence. In particular, misuse of the e-mail system or inappropriate use of the internet by viewing, accessing, transmitting or downloading any of the following material, or using any of the following facilities, will amount to gross misconduct (this list is not exhaustive):

- Accessing pornographic material (that is writings, pictures, films, video clips of a sexually explicit or arousing nature), racist or other inappropriate or unlawful materials.
- transmitting a false and/or defamatory statement about any person or organisation.
- sending, receiving, downloading displaying or disseminating material which is discriminatory, offensive, derogatory or may cause offence and embarrassment or harass others.

- transmitting confidential information about the school and any of its staff, students or associated third parties.
- transmitting any other statement which is likely to create any liability (whether criminal or civil, and whether for the employee or for the school).
- downloading or disseminating material in breach of copyright.
- engaging in online chat rooms, instant messaging, social networking sites and online gambling.
- forwarding electronic chain letters and other materials.
- accessing, downloading, storing, transmitting or running any material that presents or could present a risk of harm to a child.

Any such action will be treated very seriously and may result in disciplinary action up to and including summary dismissal.
Where evidence of misuse is found the school may undertake a more detailed investigation in accordance with our Disciplinary Policy, involving the examination and disclosure of monitoring records to those nominated to undertake the investigation and any witnesses or members of management involved in the disciplinary procedure.
If necessary, such information may be handed to the police in connection with a criminal investigation.

Digital images

School ipads should be used to take images and videos of pupil; however, staff should be aware of the following guidelines:

- Photos should only be named with the pupil's name if they are to be accessible in school only. Photos for the website, Twitter or press must not include the child's name.
- The use of personal digital cameras in school is not permitted, including those which are integrated into mobile phones.

File Storage

Staff members have their own personal area on the network, as well as access to shared network drives. Any school related work should be stored on one of these network drives. Personal files are not permitted on the network areas. Staff are responsible for ensuring they have rights for the storage of any file in their area, for example copyright music files. Any files stored on removable media must be stored in accordance with the information access and security policy, summarised as follows:

- No school data is to be stored on a home computer, or un-encrypted storage device.
- No confidential, or school data which is subject to the Data Protection Act should be transferred off site unless it is sent by secure email.

Staff Mobile Phones

Mobile phones are permitted in school, with the following restrictions:

- They are not to be used when members of staff are directly supervising or working within a classroom or other area of the school. Whilst members of staff are working in the classroom they should be securely stored in a bag/cupboard/locker.
- Personal mobile phone cameras are not to be used on school trips. The school provides iPads for this purpose.
- All phone contact with parents regarding school issues will be through the schools' phones. Personal mobile numbers should not be given to parents at the school.

Social networking

- Staff members have a responsibility to protect the reputation of the school, staff and students at all times and that they treat colleagues, students and associates of the school with professionalism and respect whilst using social networking sites.

- Social networking sites should be used responsibly, and users should ensure that neither their personal or professional reputation and/or the school's reputation, nor the reputation of individuals within the school are compromised by inappropriate postings.
- Use of social networking sites for school business is not permitted, unless via the official school Twitter account @WerburghsWirral and with the permission of the IT Leader/HT.
- Members of staff will notify the HT if they consider that any content shared or posted via any information and communications technology, including emails or social networking sites conflicts with their role in the school/setting.
- No school information, communication, documents, videos and/or images should be posted on any personal social networking sites.
- No details or opinions relating to any pupil are to be published on any website.
- Users must not knowingly cause annoyance, inconvenience or needless anxiety to others (cyber bullying) via social networking sites.
- No opinions regarding another member of staff, which could cause offence, are to be posted.
- No photos or videos, which show pupils of the school who are not directly related to the person posting them, should be uploaded to any site other than the school's Website or Twitter account.
- No comment, images or other material may be posted anywhere, by any method that may bring the school or, the profession into disrepute.
- Users must not give students access to their area on a social networking site, (for example adding a student as a friend on Facebook).

Monitoring of the ICT Systems

The school may exercise its right to monitor the use of its ICT systems. This includes websites accessed, the interception of e-mail and the viewing of data stored, where it believes unauthorised use of the school's ICT system is, or may be taking place, or the system is, or may be being used for criminal purposes. Any inappropriate material found will be deleted. Monitoring software is installed to ensure that use of the network is regularly checked by the IT Leader/Technician to ensure there are no pastoral or behaviour concerns or issues of a safeguarding or prevent nature.

Other reasons for monitoring the ICT systems include the need to:

- ensure operational effectiveness of the services provided.
- maintain the systems.
- prevent a breach of the law, this policy, or any other school policy.
- investigate a suspected breach of the law, this policy, or any other school policy.

Failure to Comply with the Policy

Any failure to comply with the policy may result in disciplinary action. Depending upon the severity of the offence, a breach of this policy may be considered gross misconduct leading to summary dismissal.

Any unauthorised use of the school's ICT systems, Cloud-based ICT systems, the internet, e-mail and/or social networking site accounts, which the HT considers may amount to a criminal offence or is unlawful shall, without notice to the user concerned, be reported to the police or other relevant authority.

The school reserves the right to audit and/or suspend a user's network, e-mail and/or application account(s) pending an enquiry, without notice to the user concerned.

St Werburgh's Catholic Primary School

ACCEPTABLE USE AGREEMENT

To be completed by all staff

As a school user of the network resources/ equipment I hereby confirm that I have read and understood the Acceptable Use Policy and that I agree to follow the school rules (set out within this policy) on its use. I will use the network/ equipment in a responsible way and observe all the restrictions explained in the school acceptable use policy. If I am in any doubt, I will consult the Headteacher. I agree to report any misuse of the network to the Headteacher. Moreover, I agree to report any websites that are available on the school internet that contain inappropriate material to the Headteacher. I finally agree to ensure that portable equipment such as cameras, iPad or laptops will be kept secured when not in use and to report any lapses in physical security to the Headteacher.

Specifically, when using school devices: -

- I must not use these devices for inappropriate purposes
- I must only access those services I have been given permission to use
- I will not download, use or upload any material which is unsuitable within a school setting or that may cause disruption to the school network.

If I do not comply with the rules, I understand that this may result in loss of access to these resources as well as other disciplinary action. I realise that staff under reasonable suspicion of misuse in terms of time or content may be placed under retrospective investigation or have their usage monitored.

I understand that the school will monitor communications in order to uphold this policy and to maintain the school's network (as set out within this policy).

Signed ……. Date …….

Print name ……

Internet
Acceptable Use Policy Agreement
Permission Form

Parent/Carers Name	
Pupil Name	

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 Digital Safety and are involved in the education and guidance of young people with regard to their on-line behaviour.**

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. A copy of the Student / 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.

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, Digital 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 Digital Safety.

Signed		**Date**	

POLICY ON THE USE OF SOCIAL NETWORKING WEBSITES

The purpose of the policy is to provide clarity to all school staff on the use of any social networking website, e.g., Facebook, Twitter and its implications in relation to future employment status i.e., disciplinary action and potential dismissal. The policy relates to any young person under 19 years of age, any 'looked after child' under the age of 21 years of age, and any young person with special educational needs under the age of 24 years of age.

Any member of staff can have an account on a social networking web site however it is the responsibility of the individual to ensure that anything placed on the social networking site is appropriate and meets the standards expected of professional teachers and school support staff.

NB *School employees who have their own social networking site may have contact with relatives or family friends. However, all the requirements below would still apply to the use of Social Networking Websites.*

All school staff **must**

- Demonstrate honesty and integrity and uphold public trust and confidence in respect of anything placed on social networking web sites.

- Ensure that any content shared on any social networking web site, at any time, would be deemed as appropriate i.e., staff are personally responsible for ensuring that any privacy settings meet this requirement.

- Ensure appropriate language is used, at all times, for any comments placed on social networking sites.

- Ensure that any comments and/or images, at any time, could not be deemed as defamatory or in breach of any relevant legislation.

All school staff **must not**

- Have contact with current/ex pupils, or other children or young people where there is a relationship developed as part of their 'professional' role e.g., music tutor, on any social networking website.

- Use social networking sites as a forum to make derogatory comments which could bring the school into disrepute, including making comments about pupils, parents, other staff members, the senior leadership team, governors, local authority or the wider community.

Any breaches of this policy could result in disciplinary action and may result in your dismissal.

I understand and agree to adhere to the Policy on the Use of Social Networking Websites.

Signed	**Date**

This document has been consulted, developed and agreed by Wirral Professional Teachers Associations and Trade Unions


NUT
NASUWT
The Teachers' Union
NAHT
The Association for All School Leaders
ASCL
Association of School and College Leaders
ATL
the education union
UNISON
unite
theUNION
GMB
GMB@WORK

Camera Use Policy

Photographs and video for school and family use are a source of innocent pleasure and pride, which can enhance the self-esteem of children and young people and their families.
Parents/carers are not required to comply with the Data Protection Act 1998 when taking photographs for their own private use of their children at an organised event.
Parents should not be stopped taking photographs for their own private use because of concerns of contravening the Data Protection Act.
However, we must always be mindful of the need to safeguard the welfare of children in our school. Images may be used to harm children, for example, as a preliminary to 'grooming' or by displaying them inappropriately on the internet

This policy applies to all forms of publications: print, film, video DVD on websites and in the professional media. The media operate under their own Code of Practice. Photographs taken by the media are usually exempt from the data Protection Act

Use of Images

- The school will decide if the event is one at which photography and videoing will be permitted and inform the parents of the decision
- Only images of children suitably dressed will be allowed. Special consideration will be given to photographs taken during PE/Sports Day/Swimming
- A copy of the Camera and Video Courtesy Code will be given to all parents and will be placed on the school's website
- Parents will be prompted by a verbal announcement at the start of the event that images must be for personal use only
- People with no connection to our school will not be allowed to photograph children. Staff will question anyone they do not recognise who is using a camera and or video recorder at events and production.

Consent forms

- All parents will be asked to sign a consent form to gain permission to publish photographs in public places (including websites). Every effort will be made by the school to prevent capturing the image of any child who should not be identified.

St Werburgh's Catholic Primary School

Camera and Video Courtesy Code

A guide for parents who wish to use photography and/or video and school event.

Generally, photographs and videos taken at a school event are a source of innocent pleasure and pride. By following some simple guidelines, we can proceed safely and with regard to the law.

- Parents/Carers and others attend school events at the invitation of the Headteacher
- The Headteacher and Governing Body have the responsibility to decide if photography of school performances is permitted
- The Headteacher has the responsibility to decide the conditions that will apply so that children are kept safe, and the performance is not disrupted, and children and staff distracted. Parents and carers must follow guidance from staff as to where to stand in order to minimise disruption
- Parents and carers can only use photographs and videos taken at a school event for their personal use. Such photographs/videos must not be sold or put on the web/internet. To do so would likely break Data Protection legislation
- Parents and carers must not photograph or video children changing for performances and events
- If you are accompanied or represented by people that school staff do not recognise staff may need to check who they are before allowing them to use a camera or video recorder.

St Werburgh's Catholic Primary School

School Password Security Policy

Introduction

The school in partnership with hi-impact will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that:

- 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

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 Virtual Learning Environment (VLE).

Responsibilities

The management of the password security policy will be the responsibility of hi-impact and the Headteacher

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.

Passwords for new users and replacement passwords for existing users can be allocated by ICT Technician Any changes carried out must be notified to the manager of the password security policy (above).

Users will change their passwords regularly, when prompted by the system.

Training / Awareness

It is essential that users should be made aware of the need for keeping passwords secure, and the risks attached to unauthorised access / data loss. This should apply to even the youngest of users, even if class log-ons are being used.

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

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

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

- in ICT and / or Digital Safety lessons (the school should describe how this will take place) • through the Acceptable Use Policy Agreement

Useful Websites

ThinkUKnow
http://www.thinkuknow.co.uk/

CHILDNET
http://www.childnet-int.org/

INSAFE
http://www.saferinternet.org/ww/en/pub/insafe/index.htm

BYRON REVIEW ("Safer Children in a Digital World") http://www.dcsf.gov.uk/byronreview/

Becta

Website Digital Safety section - **http://schools.becta.org.uk/index.php?section=is**:
http://publications.becta.org.uk/display.cfm?resID=32422&page=1835
"Safeguarding Children in a Digital World"
http://schools.becta.org.uk/index.php?section=is&catcode=ss_to_es_tl_rs_03&rid=13344

KENT NGfL
http://www.kented.org.uk/ngfl/ict/safety.htm

NORTHERN GRID
http://www.northerngrid.org/ngflwebsite/esafety_server/home.asp

NATIONAL EDUCATION NETWORK
NEN Digital Safety Audit Tool: **http://www.nen.gov.uk/hot_topic/13/nen-Digital Safety-audit-tool.html**

CYBER-BULLYING
DCSF - Cyberbullying guidance
http://publications.teachernet.gov.uk/default.aspx?PageFunction=productdetails&PageMode=spectrum&ProductId=DCSF-00658-2007 Teachernet
http://www.teachernet.gov.uk/wholeschool/behaviour/tacklingbullying/cyberbullying/ Teachernet "Safe to Learn – embedding anti-bullying work in schools"
http://www.teachers.gov.uk/wholeschool/behaviour/tacklingbullying/safetolearn/
Anti-Bullying Network - **http://www.antibullying.net/cyberbullying1.htm** Cyberbullying.org - **http://www.cyberbullying.org/**

SOCIAL NETWORKING
Home Office Task Force - Social Networking Guidance - **http://police.homeoffice.gov.uk/operational-policing/crime-disorder/child-protection-taskforce** Digizen – "Young People and Social Networking Services": **http://www.digizen.org.uk/socialnetworking/** Ofcom Report:
http://www.ofcom.org.uk/advice/media_literacy/medlitpub/medlitpubrss/socialnetworking/sum mary/

Glossary of terms

AUP	Acceptable Use Policy
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
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
ISP	Internet Service Provider
LAN	Local Area Network

LSCB Local Safeguarding Children Board

MIS Management Information System

MLE Managed Learning Environment

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

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

TUK Think U Know – educational Digital Safety 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

Digital Safety Incidents

Date	Teacher/Year	Child	Incident	Reported to:	Parents Notified Yes/No