

Online Safety Policy



Approved by:

Full Governing Body

Date: March 2026

Last reviewed on:

Next review due by:

March 2027

Contents

	Page No.
1. Summary	3
2. Development/Monitoring/Review of this Policy	4
3. Scope of the Policy	5
4. Context	6
5. Policy Statements	10
6. Pupils Acceptable Use Policy Agreement	15
7. Key aspects of PREVENT	16
8. Acceptable Use Agreements/Letters	17
9. Staff/Volunteer Acceptable Use Policy Agreement	20
10. Parent/Carer Acceptable Use Policy / Online Safety Agreement	23
11. Use of Digital/Video Images	24

1. Summary

Gwladys Street Primary School firmly believes that the effective use of information and communication technologies in schools, including the use of electronic devices such as iPads and mobile technology, can bring great benefits. Recognising the online safety issues and planning accordingly will help to ensure appropriate, effective and safer use of digital technologies. We aim to educate pupils about the advantages and risks of technology and provide them safeguards to enable them to control their personal online experience.

This policy has been developed using the guidance and exemplar E-Safety policy provided by Liverpool City Council. Liverpool City Council acknowledges the support and guidance that it received from the Safer Internet Centre, The South West Grid for Learning, The UK Council for Child Internet Safety and Childnet when writing the policy.

2. Development/Monitoring/Review of this Policy

This Online Safety policy has been written and agreed by a working group made up of:

- ICT Co-ordinator – Miss L Heath
- Headteacher - Miss N Booth
- Designated Safeguarding Lead – Mrs L Upton
- Deputy Designated Safeguarding Lead – Mr I Morris
- Chair of Governors & Safeguarding Governor – Mr K Craney

Consultation with the whole school community has taken place through the following:

- Staff meetings
- School Council
- Full Governing Body meeting
- School website

This Online Safety Policy was approved by the Governing Body on:	
The implementation of the Online Safety Policy will be monitored by:	The Headteacher The Assistant Headteacher The Designated Safeguarding Lead The ICT Co-Ordinator
Monitoring will take place at regular intervals:	Each Term
The Governing Body will receive a report on the implementation of the Online Safety Policy generated by the monitoring group (which will include anonymous details of O] online incidents) at regular intervals:	Each Term
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	January 2026

Should serious online safety incidents take place, the following external persons / agencies should be informed:	Mr Ian Shackleton Education Improvement Professional New Technologies & LSIP School Improvement Liverpool
--	---

3. Scope of the Policy

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

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate online safety behaviour that take place inside and outside of school.

4. Context

We live in a digital age where technology is vastly developing and playing an ever increasing part in our lives. The internet is an essential element in the 21st Century for education, business and social interaction. The school has a duty to provide students with quality internet access as part of their learning experience. In an ever changing world, we recognise there are a widening range of issues associated with technology and a user's access to digital content, contact with others and behavioural issues. The school has a duty to ensure that all staff, pupils and parents / carers associated with the school are able to use technology in a safe and responsible manner.

Some of the potential dangers of using technology may 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 with 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 offline world but it is important that as a school we have a planned and coordinated approach to ensuring that all involved with the school use technology in a safe and responsible way. As with all risks, it is impossible to eliminate them completely but with a planned and coordinated approach they can be significantly reduced and users can be taught to manage them effectively.

Gwladys Street Primary School has adopted the PIES model which is the basis of its approach towards Online Safety and helps to manage and minimise its risk.



1) Policies and practices

The Online Safety policy outlines the importance of ICT within and outside of education. It provides guidance on the schools approach to Online Safety and details a code of conduct for school staff and pupils. The policy aims to provide an agreed, coordinated and consistent approach to Online Safety. The code of conduct forms the basis of the schools expected behaviours regarding the use of technology and any infringements of the code of conduct will lead to disciplinary action against the perpetrator(s).

2) Infrastructure and technology

As of September 5th September 2016, the school has been planning and implementing the DFE's revised statutory safeguarding advice for schools and maintained nurseries. As part of this process, we are ensuring the school has appropriate filtering and monitoring systems in place.

At Gwladys Street, our school network and access to the internet is provided by Liverpool City Council through its IT partner **MGL World (MGL)**. This network provides a safe and secure 10Mbps broadband connection to the internet via the LDL data centres. There is a multi-layer security shield that provides dual-layer firewall protection, intruder detection/prevention, load balancing, content caching, data traffic analysis and virus protection. There is a cloud-based filtering service, **SENSO**, which filters internet content using the City Councils base policy. **SENSO** undertakes live scanning of all sites and blocks any threats or inappropriate websites. The infrastructure has been designed to minimise the risk of; users accessing inappropriate material, data being lost or accessed by unauthorised users, virus or malware threats. At present, we are in the process of updating our network and broadband system. We will be ensuring all internet and network activity is logged via the LDL data centre and can be retrieved if required in the event of an investigation.

The school is responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible. This will be implemented in the following ways:

Managing Internet Access

– Information system security:

- The security of the school information system will be reviewed regularly with advice from technology specialists.
- Virus protection will be installed and updated regularly
- The school uses broadband with its firewall and filters

– Email:

- Pupils may only use approved email accounts on the school system. Children are not allowed access to personal email accounts or chat rooms whilst in school.
- Pupils must immediately tell a teacher if they receive offensive email.
- Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone with specific permission.

– Published content and the school website:

- The contact details on the website should be the school address, email and school telephone number. Staff or pupils personal information will not be published.
- The senior leadership team will take overall editorial responsibility and ensure that published content is accurate and appropriate

3) Education and training

As the use of technology and the potential risks associated with the use of the technology change rapidly, it is essential to ensure that the school community know how to use technology safely and responsibly. The school is committed to ensuring that staff receive regular training to keep up to date with new developments and ensure that they are sufficiently confident to educate pupils in the safe and responsible use of technology.

As well as staff, the education of pupils in online safety is an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Our Online Safety Provision will be provided in the following ways:

- In partnership with MGL, the school have designed a Computing Curriculum that incorporates online safety throughout each year group and is regularly taught. Pupils are 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;
- Key online-safety messages should be reinforced as part of a planned programme of assemblies;

- If staff or pupils discover unsuitable sites, the, computer / electronic device number, URL (website address), time, date and content must be reported to the school Computing Co-ordinator.
- Pupils should be helped to understand the need for the Pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school;
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices;
- Where students / pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

The curriculum is reviewed and revised on a regular basis to ensure that it remains current. The school will also endeavour to provide information and training opportunities for parents and carers to raise their awareness of the technologies that their children are potentially use, and the risks that they potentially face.

4) Standards and inspection

The school reviews its approach to Online Safety on a regular basis. Reference is also made to online safety through Ofsted inspections.

5. Policy Statements

Whilst the PIES model forms the basis of the schools approach to Online Safety, the school will ensure that all access to the internet and ICT systems by pupils is effectively managed and supervised.

As part of the Online Safety policy the school will also manage:

- **The use of digital images and video – refer to “Safe use of AI” policy**
- Data protection
- Digital communications and social networking
- Emerging technologies
- Authorising Internet access
- Unsuitable/inappropriate activities
- Incidents of misuse

The use of digital images and video

School staff and pupils are made aware of the potential risks associated with storing, sharing and posting images on the internet and must follow the good practice detailed below.

- When using digital images, staff will inform and educate pupils about the risks associated with the taking, using, sharing, publishing and distributing images. In particular, they will recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Staff are permitted to take digital images and video 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 will be taken when capturing digital images and video that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Images and videos published on the school website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.

- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Pupil's work will only be published with the permission of the pupil and parents or carers.

Data Security and 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.

All school staff will ensure that:

- Care is taken to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Personal data is used or processed on only secure password protected computers and other devices and that these devices are properly "logged-off" at the end of any session in which they are using personal data.
- Data is transferred securely using encryption and secure password protected devices and email solutions.
- 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

Digital Communication & Social networking

Digital communication is an area that is developing rapidly with new and emerging technologies, devices are becoming more mobile and information sharing/communication is becoming more sophisticated.

When using communication technologies the school ensures the following good practice:

- The official school email service is 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, on school business or on school systems.
- Users need to be aware that email communications / social networking messages may be monitored
- Users must immediately report 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, pupils or parents/carers (email, chat, VLE 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 will 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.
- Social networking sites will be blocked unless a specific use is approved.
- Pupils and parents will be advised that the use of social networking sites outside of school may be inappropriate for primary aged pupils.

Managing emerging technologies

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

Mobile phones and electronic equipment should not be brought into school unless permission is given for special circumstances and parents are aware that school is not liable if they become lost.

Authorising Internet access

- The school will maintain a current record of all staff and pupils who are granted internet access.
- All staff must read and sign the Acceptable User Policy (AUP) before using any school computing resource.
- At FS / KS1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved online materials.

- Parents and pupils will be asked to discuss the content with their child, sign and return a consent form agreeing to comply with the school's Acceptable Use Policy.

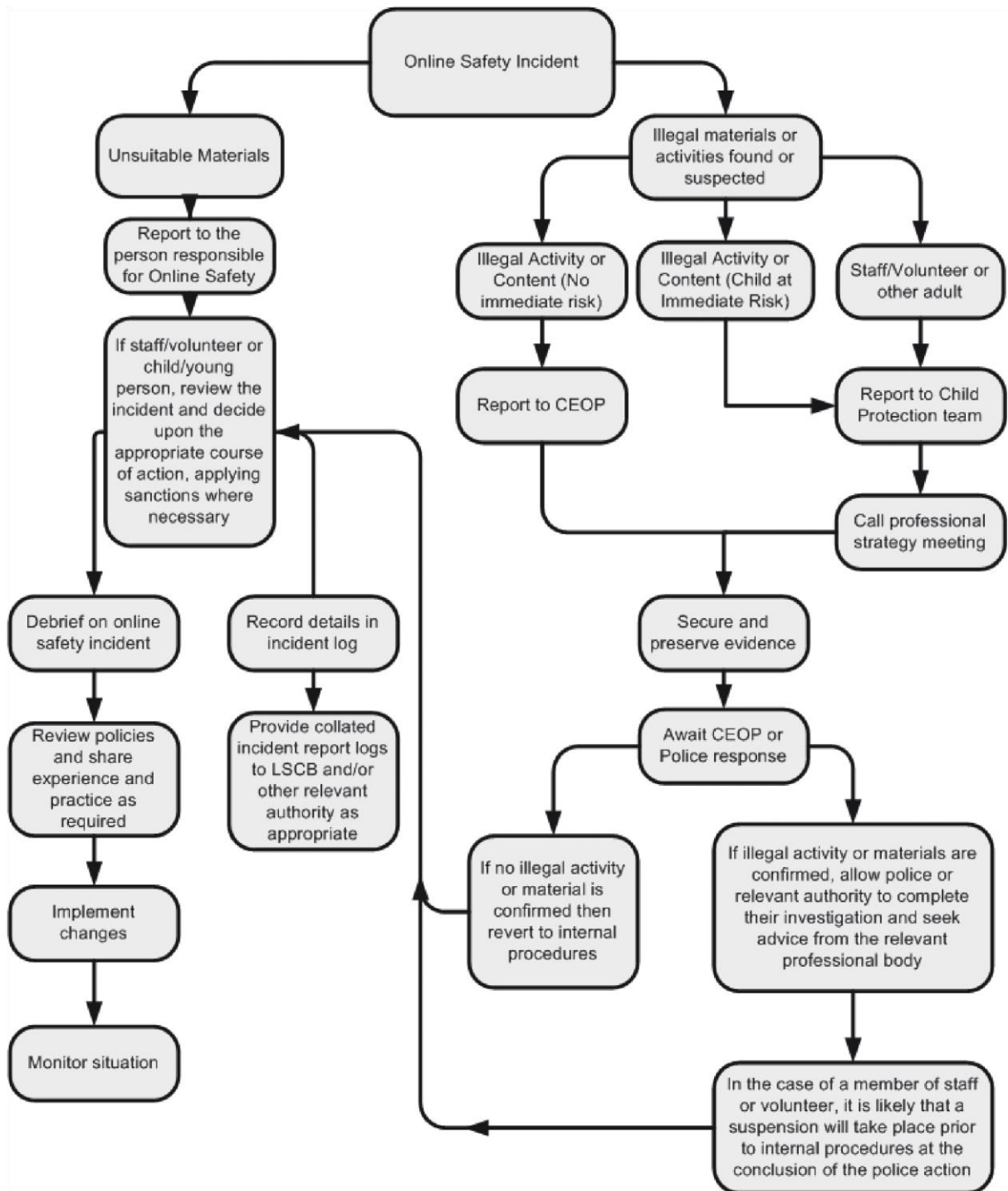
Unsuitable/inappropriate activities

School ICT systems are only to be used for agreed, appropriate and suitable work related activities. Internet activity which is considered unsuitable or inappropriate will not be allowed and if discovered will lead to disciplinary action. Internet activity which is illegal will be reported and could lead to criminal prosecution.

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 accidentally, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of an online safety incident it is important that there is a considered, coordinated and consistent approach. Incidents will be managed using the incident flowchart below.



All incidents will be recorded and reported to the relevant parties and organisations.

6. Pupils 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.

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.

7. Key aspects of PREVENT

- **Online Risks:** Misinformation, disinformation, and conspiracy theories are explicitly highlighted as safeguarding harms.
- **Online Safety:** Schools must equip pupils with critical thinking skills to challenge online content and protect against manipulation.
- **AI Risks:** Guidance includes addressing harmful imagery and content potentially generated by artificial intelligence. Ensure filtering and monitoring systems are robust against AI-generated content.
- **Curriculum Updates:** Computing curricula should be regularly reviewed and updated where necessary to cover these new digital risks and media literacy.
- **Prevent Activities:** The DSL and IT Co-Ordinator oversees Prevent activities, ensures filtering/monitoring systems address new risks, and conducts risk assessments. Also to monitor and address any issues raised by the Filtering System, SENSO.
- **Contextual Safeguarding:** Risks from broader environments (neighbourhoods, online) must be assessed, with termly reviews by the DSL & IT Co-Ordinator
- **Changes to the KCSIE 2025 document** - incorporates changes reflecting current online threats, expanding on previous guidance.

Gwladys Street Community Primary & Nursery School

EYFS/KS1 Pupil 'Use of Technology' Agreement

Acceptable Use Policy Agreement (to be read out to pupils)

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.

Online Rules:

For my own personal safety:

- I will ask an adult if I want to use the computer.
- I will only use activities that an adult says are OK.
- I will take care of the computer and other equipment.
- I will ask for help from an adult if I am not sure what to do or if I think I have done something wrong.
- I will tell an adult if I see something that upsets me on the screen.
- I will be aware of "stranger danger", when I am communicating on-line.
- I know that if I break the rules I might not be allowed to use a computer.
- I understand these computer rules and will do my best to keep them.

My Name: _____

Class: _____

Date: _____

Gwladys Street Community Primary & Nursery School

KS2 Pupil 'Use of Technology' Agreement

Acceptable Use Policy Agreement (to be read out to pupils)

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.

Online Rules:

For my own personal safety:

- I will only use technology in school to support my learning.
- I will not tell other people my personal information, including passwords and usernames.
- I will only open and delete my own files.
- I will make sure that all my technological contact with other children and adults is responsible, polite and sensible.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this, I will tell my teacher immediately.
- I will not give out my own details such as my name, phone number or home address.
- I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult accompanies me.
- I am ultimately responsible for my behaviour when using technology, no excuse. I know that these rules are to keep me safe.
- I understand that I am responsible for my actions using online games at home and will remember online safety rules discussed here and in school and follow them.
- I will not deliberately upload or add any images, video, sounds or text that could upset any member of the school community.
- I know that my use of technology can be checked and that my parent/ carer will be contacted if a member of school staff is concerned about my eSafety. I will take care of the computer and other equipment.

My Name: _____ Class: _____ Date: _____

Gwladys Street Community Primary & Nursery School

Walton Lane

Liverpool

0843

L4 5RW

1453

Headteacher: Miss N Booth B.A. Hons, PGCE, NPQH

www.gwladysstreet.org

Tel: 0151 525

Fax: 0151 530

Dear Parent/ Carer,

ICT including the internet, email, mobile and gaming technologies, etc continues to become an even more important part of learning in our school and social interactions at home. We expect all children to be safe and responsible when using all technology platforms.

We have created a list of guidelines which children at Gwladys Street must adhere to in order to keep our school community safe. Please read and discuss the above online safety rules with your child and return the slip at the bottom of this page.

If you have any concerns or would like some explanation, please contact Mrs Upton or Miss Heath.

It is our priority to ensure Gwladys Street children feel safe and use the internet and all technology platforms safely.

.....

We have discussed this and (child name) agrees to follow the online rules set out above and to support the safe use of technology at Gwladys Street Primary.

Parent/ Carer Signature

Class Date



7. Staff/Volunteer 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. 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 students / pupils learning and will, in return, expect staff and volunteers to agree to be responsible users.

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 e-safety 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, VLE 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 / VLE) 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 on-line 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 not use personal email addresses on the school ICT systems.
- 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 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 _____

8. Parent/Carer Acceptable Use Policy / Online Safety Agreement

Gwladys Street Community Primary School & Nursery School

Parent / guardian name:

Pupil name:

Pupil's class:

As the parent or legal guardian of the above pupil(s), I grant permission for my child to have access to use the Internet, school Email and other technological facilities at school.

I know that my daughter or son has signed a form to confirm that they will keep to the school's rules for responsible technology use and understand that my son/daughter may be informed if the rules have to be changed during the year. I know that the latest copy of the e-Safety Policy is available from the school office or on the school website and that further advice about safe use of the Internet can be found it the school's website.

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school will take every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. These steps include using a filtered internet service, secure access to email, employing appropriate teaching practice and teaching e-safety skills to pupils.

I understand that the school can check my child's computer files, and the Internet sites they visit. I also know that the school may contact me if there are concerns about my son/daughter's online safety or online behaviour.

I will support the school by promoting safe use of the Internet and digital technology at home and will inform the school if I have any concerns over my child's online safety.

Parent's signature:..... Date:.....

9. Use of Digital/Video Images

The use of digital/video images plays an important part in learning activities. Students / Pupils and members of staff may use digital cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons.

Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media.

The school will comply with the Data Protection Act and request parents / carers permission before taking images of members of the school. We will also ensure that when images are published that the young people cannot be identified by the use of their names.

Although the paragraph outlined (in blue italics) below may be used in future Acceptable Use Agreements with parents/carers, we currently ask the parent/carer to sign a separate (Pink Form) form to either grant/withdraw permission to allow the school to take and use digital/video images of their children. The outcome for each child has been collated and distributed to all members of staff within the school.

Gwladys Street Primary School also ensures that any visitor(s) who requests the use of digital/video images are advised of the policy, and that any digital/video images are checked prior to their departure from the school premises.

Permission Form

Parent/Carers Name

Pupil Name

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

*I agree that if I take digital or video images at, or of, – school events which include images of children, other than my own, I will abide by these guidelines in my use of these images and I **will not publish any images onto social media sites.***

Signed

Date
