Carnalridge Primary School

E-Safety Policy

NAME:	ROLE:
Jade Thorne	Principal
Andrew Bingham	Chair of Board of Governors

Date Ratified:	**10th June 2024**
Date of Review:	June 2025

Rationale

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. A school e-safety policy should help to ensure safe and appropriate use. The development and implementation of such a strategy should involve all the stakeholders in a child's education from the Principal and Governors to the senior leaders and classroom teachers, support staff, parents, members of the community and the pupils themselves.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil / student achievement.

However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

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

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

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

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 e-safety policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents / carers) to be responsible users

and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

Schedule for Development / Monitoring / Review

This e-safety policy was approved by the *Governors on:*	*10th June 2024*
The implementation of this e-safety policy will be monitored by the:	*ICT Co-Ordinator and Principal*
Monitoring will take place at regular intervals:	*Yearly*
The *Governors* will receive a report on the implementation of the e-safety policy:	*Yearly*
The E-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 esafety or incidents that have taken place. The next anticipated review date will be:	*June 2025*
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	*PSNI, CPSSS*

Scope of the Policy

This policy applies to all members of the school community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of 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 school will deal with such incidents within this policy and associated behaviour and antibullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the roles and responsibilities for e-safety of individuals and groups within the school:

Governors:

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the *Governors* receiving regular information about e-safety incidents and monitoring reports.

Principal and Senior Leaders:

- **The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community**, though the day to day responsibility for e-safety will be delegated to the *E-Safety Co-ordinator*.
- *The Principal / Senior Leaders are responsible for ensuring that the E-Safety Coordinator and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant*
- **The Headteacher and another member of the Senior Leadership Team / Senior Management Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.** (see SWGfL flow chart on dealing with e-safety incidents – included in a later section – "Responding to incidents of misuse" and relevant Local Authority HR / disciplinary procedures)

E-Safety Coordinator:

- leads the e-safety committee
- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority
- receives reports of e-safety incidents and creates a log of incidents to inform future esafety developments

ICT Co-ordinator:

The ICT Co-ordinator is responsible for ensuring:

- **that the school's ICT infrastructure is secure and is not open to misuse or malicious attack**
- **that the school meets the e-safety technical requirements outlined in any relevant Local Authority ESafety 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**
- C2k is informed of issues relating to the filtering applied by the Grid
- that he / she keeps up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- that the use of the *network / Virtual Learning Environment (VLE) / remote access / email* is regularly monitored in order that any misuse / attempted misuse can be reported to the *E-Safety Co-ordinator for investigation / action / sanction*
- *that monitoring software / systems are implemented and updated as agreed in school policies*

Teaching and Support Staff

are responsible for ensuring that:

- **they have an up to date awareness of e-safety matters and of the current school esafety policy and practices**
- **they have read, understood and signed the school Staff Acceptable Use Policy (AUP)**
    - **they report any suspected misuse or problem to the E-Safety Co-ordinator for investigation / action / sanction**
- **digital communications with students / pupils (email / Virtual Learning Environment (VLE) / voice) should be on a professional level** *and only carried out using official school systems*
- e-safety issues are embedded in all aspects of the curriculum and other school activities
- students / pupils understand and follow the school e-safety and acceptable use policy
- students / pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor ICT activity in lessons, extra curricular and extended school activities
- they are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices
- *in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches*

Child Protection Officer

should be trained in e-safety issues and be aware of the potential for serious child protection issues to arise from:

- sharing of personal data

- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

Parents / Carers

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

- **endorsing (by signature) the Student / Pupil Acceptable Use Policy**
- accessing the school website / VLE / on-line student / pupil records in accordance with the relevant school Acceptable Use Policy.

Community Users

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

Policy Statements

Education – pupils

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

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

Education – parents / carers

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's 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, web site, Class Dojo*
- *Parents information sessions*
- *Reference to the Safer Schools App*

Education & Training – Staff

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

- **All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policies**
- *This E-Safety policy and its updates will be presented to and discussed by staff in staff meetings*
- *The E-Safety Coordinator will provide advice / guidance / training as required to individuals as required*

Training – Governors

Governors should take part in e-safety training / awareness sessions. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority through the SDS portal
- Participation in school training / information sessions for staff or parents

Technical – infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that c2k maintain the school network, ensuring it is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their esafety responsibilities:

School ICT systems will be managed in ways that ensure that the school meets the esafety technical requirements outlined by relevant Local Authority E-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.** *Details of the access rights available to groups of users will be recorded by the Network Manager (or other person) and will be reviewed, at least annually, by the Principal.*
- **All users will be provided with a username and password** by *school who will keep an up to date record of users and their usernames. Users will be required to change their password every 3 months*
- *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 C2k*
- *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 C2k*

- *Requests from staff for sites to be removed from the filtered list will be considered by the Principal. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the E-Safety Co-Ordinator.*
- *An appropriate system is in place for users to report any actual / potential e-safety incident to the Principal.*
- *The school infrastructure and individual workstations are protected by up to date virus software.*
- *Personal data can not be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.*

Curriculum

E-safety should be a focus in all areas of the curriculum and staff should reinforce esafety 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, eg using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.*
- *Students / 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*
- *Students / pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.*

Use of digital and video images - Photographic, Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and 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. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- **When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.**
- *Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.*
- *Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.*
- *Pupils must not take, use, share, publish or distribute images of others without their permission*

- *Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.*
- *Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.*
- *Written permission from parents or carers will be obtained before photographs of pupils are published on the school website (this is covered as part of the AUP signed by parents or carers at the start of the year*
- *Pupil's work can only be published with the permission of the pupil and parents or carers.*

Data Protection

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

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

Staff must ensure that they:

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

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

- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

Communications

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

	Staff & other adults				Students / Pupils			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	**X**						**X**	
Use of mobile phones in lessons				X				X
Use of mobile phones in social time		X						X
Taking photos on mobile phones or other camera devices		x						X
Use of personal email addresses in school, or on school network			x					X
Use of school email for personal emails	X							X
Use of chat rooms / facilities				X				X
Use of instant messaging		X						X
Use of social networking sites			X					X
Use of blogs		X				X		

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

- The official school filtering service may be regarded as safe and secure and is monitored. *Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (eg by remote access).*
- Users need to be aware that email communications may be monitored
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.

- **Any digital communication between staff and students / pupils or parents / carers (email, chat, Class Dojo 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.*
- *Whole class or group email addresses will be used at KS1, while pupils at KS2 and above will be provided with individual school email addresses for educational use.*
- *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.*

User Actions: Unsuitable / inappropriate 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:

		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	**child sexual abuse images**					X
	promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation					X
	adult material that potentially breaches the Obscene Publications Act in the UK					X
	criminally racist material in UK					X
	pornography				X	
	promotion of any kind of discrimination				X	

	promotion of racial or religious hatred				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	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				X	
Using school systems to run a private business					X	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by c2K and / or the school					X	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions					X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
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					X	
On-line gaming (educational)			x	x		
On-line gaming (non educational)					x	
On-line gambling					x	
On-line shopping / commerce			x	x		

File sharing			x		
Use of social networking sites			x		
Use of video broadcasting eg Youtube			x		

Handling E-Safety Complaints

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities.

- Parents, teachers and pupils should know how to submit a complaint.
- A range of sanctions will be required when rules are breached, linked to the school's disciplinary policy.

Illegal Incidents

- If there is any other suspected illegal activity, report to the Safeguarding team.
- If the school identifies a suspect computer (containing for instance indecent images or offences concerning child protection), it should **not** be used or viewed. Schools should isolate any devices concerned and take advice from local police.
- **In some circumstances such interference may also constitute a criminal offence. Potential child protection or illegal issues must be referred to the school Designated Child Protection Coordinator or Safeguarding team.**

After a major or minor incident, a comprehensive debriefing should occur to review school policy and procedures, to make and monitor any necessary changes and to maximise what can be learnt.

- Complaints of Internet misuse will be dealt with by the Safeguarding team.
- Any complaint about staff misuse must be referred to the designated teachers for child protection.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure.

School Actions and Sanctions - Pupils

Incidents:	Refer to class teacher / tutor	Refer to Safeguarding Team	Refer to Headteacher	Consider Referral to PSNI	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg reflection /
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X		X			
Unauthorised use of non-educational sites during lessons	X							X	
Unauthorised use of mobile phone / digital camera / other handheld device	X					X		X	
Unauthorised use of social networking / instant messaging / personal email	X					X		X	
Unauthorised downloading or uploading of files	X					X		X	
Allowing others to access school network by sharing username and passwords	X							X	
Attempting to access or accessing the school network, using another student's / pupil's account	X							X	
Attempting to access or accessing the school network, using the account of a member of staff			X	X	X	X			X
Corrupting or destroying the data of other users			X	X		X			X
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature			X	X		X			X
Continued infringements of the above, following previous warnings or sanctions			X	X		X	X		
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school			X			X			X
Using proxy sites or other means to subvert the school's filtering system			X	X	X	X	X		
Accidentally accessing offensive or pornographic material and failing to report the incident		X	X		X	X			

Deliberately accessing or trying to access offensive or pornographic material		X	X	X	X	X	X		
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act		X		X				X	

School Actions and Sanctions - Staff

Incidents:	Refer to Safeguarding Team	Refer to Principal	Refer to C2k	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X				
Inappropriate personal use of the internet	X					X		
Unauthorised downloading or uploading of files	X					X		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	X					X		
Careless use of personal data eg holding or transferring data in an insecure manner	X					X		
Deliberate actions to breach data protection or network security rules	X	X	X					
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X	X	X					
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	X	X						
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	X	X						
Actions which could compromise the staff member's professional standing	X	X						
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X	X						
Using proxy sites or other means to subvert the school's filtering system	X	X	X		X	X		
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X	X		X			
Deliberately accessing or trying to access offensive or pornographic material	X	X	X		X			
Breaching copyright or licensing regulations	X	X						
Continued infringements of the above, following previous warnings or sanctions	X	X						

Addendum

- The E-safety Co-ordinator and the Principal reserve the right to review files and communications to maintain system integrity and ensure that the users are using the system responsibility – they will respect the right to privacy whenever possible

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor C2k can accept liability for the material accessed, or any consequences of Internet access.

- The school will audit ICT provision to establish if the E-Safety policy is adequate and that its implementation is effective.

CPS Pupil User Agreement

This Acceptable Use Agreement is intended to ensure that pupils will be responsible users and stay safe while using the internet and other digital technologies for educational use.

- I will access the system with my own username and password which I will keep safe and secure;
- I will not access other people's files;
- I will only use the computers and tablet devices for school work and homework;
- I will not bring in data pens from outside school unless I have been given permission;
- I will ask permission from a member of staff before using the Internet;
- I will only e-mail or message people I know, or my teacher has approved;
- The messages I send will be polite and responsible;
- I will not give my home address or telephone number, or arrange to meet someone, unless my parent or carer has given permission;
- I will follow the rules and guidelines that my teacher has discussed with the class.
- I will not open e-mails or messages sent by anyone we don't know;
- I will report any unpleasant material or messages sent to me.
- I will only use search engines in the presence of a teacher or another adult in school;
- I will immediately close any webpage I am not sure about;
- I will not use Internet chat rooms or social media accounts.

- I understand that the school may check my computer/device files and may monitor the Internet sites I visit;
- I understand that irresponsible use may result in the loss of network or Internet access.
- I understand that all personal mobile /camera phones must be switched off during school;
- I understand that if using information from the Internet I must include the web address.

Signed: Date: _____

Carnalridge Primary School

Safe and Effective Use of the Internet

Agreement & Consent Form

All pupils use computer facilities including Internet access as an essential part of learning, as required by the Northern Ireland Curriculum. Both pupils and their parents/carers are asked to read the rules and sign to show that these have been understood and agreed.

Pupil:	***Class:***

Pupil's Agreement

I have read and I understand the Rules for Safe Use of Internet.
I will use the computer, network, mobile phones, Internet access and other new technologies in a responsible way at all times.
I know that network and Internet access may be monitored.

Signed:	***Date:***

Parent's Consent for Internet Access

I have read and understood the school E-Safety rules and give permission for my son / daughter to access the Internet. I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials but I appreciate that this is a difficult task.
I understand that the school cannot be held responsible for the content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities.

Signed:	***Date:***

Parent's Consent for Web Publication of Work and Photographs

I agree that my son/daughter's work may be electronically published. I also agree that appropriate images that include my son/daughter may be published subject to the school rule that photographs will not be accompanied by pupil names.

Signed:	***Date:***

Please print name:

Please complete, sign and return to school.

Staff/Volunteer Information Systems Code of Practice

To ensure that staff are fully aware of their professional responsibilities when using information systems, they are asked to sign this code of conduct. Staff should consult the school's 'Safe Use of Internet and Digital Technologies' policy for further information and clarification.

- The information systems are school property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.
- I will ensure that my information systems use will always be compatible with my professional role.
- I understand that school information systems may not be used for private purposes, without specific permission from the principal.
- I understand that the school may monitor my information systems and Internet use to ensure policy compliance.
- I will not disclose any password or security information to anyone other than an appropriate system manager.
- I will not install any software or hardware without permission.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the school ICT Coordinator or the Designated Child Protection Teacher.
- I will ensure that any electronic communications with pupils are compatible with my professional role.
- I understand that staff members may use personal digital devices on field trips; any images should be appropriately transferred back to a centralised area in the staff public folder and deleted that day.
- I will promote E-Safety with students in my care and will help them to develop a responsible attitude to system use and to the content they access or create.
- I will adhere to Use of Social Media guidelines as set out in Use of Internet and Digital Technologies Policy/ Social Media Policy. The school may exercise its right to monitor the use of the school's information systems, including Internet access, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read, understood and agree with the Information Systems Code of Conduct.

Signed: ..... Date: .....