Pray, Learn, Achieve and Celebrate Together

Acceptable Use Policy

"For I know the plans I have for you," says the Lord..."plans to give you Hope and a Future."
Jeremiah 29:11

Written: September 2022

Section One

Introduction

Computing in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment. Computing covers a wide range of resources including; web-based and mobile learning. It is also important to recognise its constant and fast paced evolution within our society as a whole.

Information and communication technologies, systems and services are a pivotal part of school life in St. Gabriel's. They are required to support staff, visitors and children alike.

The aim of this policy is to clearly define what the school considers to be acceptable, unacceptable and forbidden use of its technologies, systems and services. It is not designed to make unnecessary restrictions and its ultimate goal is for the people and technologies to remain safe.

The services covered in this policy will include:

- System/applications
- The internet
- E-mail
- Mobile devices (cameras, phones, whiteboards etc.) Landline telephones
- Personal Computers
- Laptops
- Tablets .
- Servers
- Any other technology devices (projectors, green screen software etc.)
- Social Media

Who does this policy apply to?

This policy applies to all pupils, staff, parents and visitors of the school. It also extends to any users accessing information from a remote location.

The responsibilities of the school

In partnership with ABtec Computer Solutions Ltd, the school is responsible for ensuring that its systems, technologies and data held on them is secure. In addition to this, the school is responsible for promoting reasonable and legitimate computing use. As a result of this, the school reserves the right to monitor maintain and keep records of people's use of these services. Those using the services need to be aware that the school's monitoring system will stores a record of user activity and that this activity can be viewed for monitoring purposes. These messages may also be subject to disclosure under the Freedom of Information Act.

Your responsibilities

All users of the schools computing services are responsible for safe, secure, professional and lawful use of them. Users must take care of devices supplied and in addition to this any data held on them. This includes protecting them from damage, theft or loss. In the event of preventable damage, theft or loss, a charge to you may be incurred in order to replace such technologies. Finally all users are responsible for ensuring that they have fully read and understood this policy. If you have any queries regarding anything in this policy please refer to the Headteacher or the schools Computing Coordinator.

Headteacher responsibilities

It is the Headteacher's responsibility to ensure that:

- All staff have read and signed this policy
- Children and their parents/main carers have read and signed the children's contract. .
- That all visitors who use these technologies have read and signed this policy.
- The policy is reviewed every three years or before where new technologies have been developed.
- The policy is refreshed in staff meetings on an annual basis.
- The policy is explained during new staff inductions.

Definitions in this policy

This code of practice outlines the school's view on what is deemed acceptable use, unacceptable use and use which is expressly forbidden At all times parties using the technologies and systems must abide by the protocols set out in this and any laws pertaining to the secure use of data, devices and technology systems and services.

Users should also abide by protocols set out in:

- Saint Gabriel's e Safety policy
- Saint Gabriel's Safeguarding policy
- Saint Gabriel's Code of Conduct
- Wigan Councils Social Media Policy for Employees in Schools.

Any activity that the school refers to as acceptable use is one which is permitted for authorised users of ICT within the school. It is in place to help and support users to further their roles within the school

Any activity that the school refers to as unacceptable use would be a breach of this policy and the schools code of conduct. Unacceptable use may face disciplinary action, and this action could be classified as gross misconduct in extreme circumstances (e.g. long periods of misuse, repeated and persistent breaches, the volume of offences)

Any activity that the school refers to as forbidden is anything which is deemed to be a breach of safe and secure use. It would be considered to be in full breach of this policy and the schools code conduct. This would result in automatic disciplinary action and in many cases would classify as gross Misconduct Employee dismissal and civil and criminal proceedings may occur at this level.

WARNING: If you are unsure whether something constitutes unacceptable or forbidden use please seek advice from the Headteacher before undertaking the task.

Section Two

Acceptable Use of St. Gabriel's Primary School Systems and Services

The information in these sections clarities what the school deems to be acceptable. unacceptable and forbidden use of its technologies and systems.

This document serves as a guideline and the examples used are **not exhaustive** of what constitutes acceptable, unacceptable and forbidden use

The information in this section is broken down into the following sub-headings:

- Internet services
- Use of E-mail
- Use of software
- Use of electronic equipment .
- Use of user accounts and passwords
- Use of telephones
- Guidance for staff and visitors.

Internet Services

We define the following as acceptable internet use in school:

- Accessing Education related websites in relation to the user's job.
- Accessing business related websites in relation to the user's job.
- Using online video clips to educate - provided the content of the clips have been thoroughly checked by the user prior to sharing them.
- Downloading and using safe and secure files that are not subject to copyright laws.
- Accessing personal e-mails, websites and social media in the designated area (the staff room)
    - on your mobile phone
    - using your own internet connection

We define the following as unacceptable internet use:

- Using the schools internet service for personal use
- Providing your work e-mail address to websites for non
- business related purposes.
- Downloading any copyright material without the owner's permission
- Connecting your personal devices to the schools internet connection

We define the following as forbidden internet use:

- Using web based e-mail and social media outside the designated areas or on work equipment (e.g. Facebook Gmail, etc.)
- Downloading software used for hacking or cracking passwords
- Making repeated attempts to access websites that have been blocked by the schools web filtering software.
- Entering your password to override the filtering system on a pupil account (where you feel a site has been unnecessarily blocked please contact the Computing Coordinator)
- Using the school's internet to access non-business or education related activity during working hours. (e.g.

Using them for Live Sports new feeds, downloading images, videos or audio streams for personal use)

- Accessing sites containing pornographic, offensive, racist or obscene material that may cause offence to others .
- Using someone else's personal user account to access the
- internet.
- Attempting to bypass or avoid any of the school's security **features.**

WARNING It is important to note that the list above is not all encompassing and any other use that may be a security risk, detrimental to children's wellbeing or highly unprofessional would be subject to consequences.

E-mail Services

We define the following as acceptable e-mail use in school:

- Communication in relation to the schools education and business.
- Headteacher accessing users mail box(es), where there is a legitimate need (e.g. a person is absent and an important e mail is expected)
- Limited use of e-mail internally only for non-business purposes outside of working hours (e.g. organising to go out for a meal with colleagues)
- Using the e-mails OneDrive to store planning and resources. (provided initials only are used)

We define the following as unacceptable e-mail use:

- Customising e-mail with non-school logos, backgrounds or signatures
- Forwarding chain e-mails.
- Sending work related information to and from your personal e mail address.

We define the following as forbidden e-mail use:

- Sending messages or files that contain discriminatory. abusive, racist, pornographic, obscene, illegal, offensive, potentially libellous or defamatory content.
- Supplying your work e-mail for non-business related purposes (e.g. Facebook, Amazon, EBay).
- Using the e-mails OneDrive to store sensitive data (e.g. anything that contains pupil names or data, any confidential information pertaining to staff and visitors). Sending sensitive data (as listed) to personal e-mail accounts or to unauthorised external recipients.
- Excessive use of e-mail to internal personal for non-business purposes.
- Sending e-mails from another users e-mail account.
- Use of school e-mail to send personal messages to external sources (e.g. family and friends etc.)

- E-mailing private and confidential information to others (internally or externally) without ensuring that it is secure and protected
- Sending files with non-business related attachments. (i.e images, videos, streams, compressed files, executable codes)

- Using web based e-mail services on school devices (i.e. Facebook Mail, G Mail etc.)

PLEASE NOTE: Unsolicited receipt of discriminatory, abusive, racist, pornographic obscene, illegal offensive and defamatory emails will not result in disciplinary action. However please ensure that any instances of this are reported immediately to the Headteacher and Computing Coordinator if it is from an unknown source then the message must be deleted without a message being sent back to the originator

In addition where you receive content of this nature from a known sender, whether you find it offensive or not, you must inform them that you do not want to receive this kind of information and report the content to the Headteacher.

WARNING It is important to note that the list above is not all encompassing and any other use that may be a security risk, detrimental to children's wellbeing or highly unprofessional, would be subject to consequences.

Use of Electronic Equipment

The school defines, but does not limit, electronic equipment to include

- Staff and pupil Laptops
- Class and Pupil Tablets
- PC's
- Projectors
- Interactive Whiteboards
- Curriculum resources (e.g. Science data loggers/Bee Bots etc.)
- Security devices (i.e. Fobs for the doors and gates)
- Servers Chargers and cables

All users must ensure that they protect all electronic equipment from damage, loss and theft. In the event of preventable damage, theft or loss a charge may be applied.

We define the following as acceptable use of electronic equipment in school

- Ensuring data created, uploaded and stored is done so
- securely and backed up
- Ensuring staff laptops are encrypted prior to being used.
- Hand held devices such as tablets being password protected
- Only loading text, images, videos, or audio streams that are for business use.
- Equipment and resources being properly stored (e.g. in their protective casings, in their designated space with no risk of damage)
- Laptops, tablets and any device that holds personal data being secured in locked cabinets and rooms overnight
- Staff laptops which are permitted to leave the building, being transported and stored in a secure manner (e.g. not left in a car overnight or in view while vehicle is unattended, stored in the home in a place which is not easily accessible or prone to being damaged)
- Equipment being handled and used in a respectful way that safeguards against damage.

We define the following as **unacceptable** use of electronic devices:

- Incorrectly storing any electronic equipment (e.g. in a place where it may fall or be damaged by a third party)
- Careless handling or use of equipment (e.g. allowing food and liquids near laptops, rough handling of equipment, not checking that charging leads are out of the way before shutting doors on laptop banks)
- Not transporting and storing school equipment appropriately at home (transporting laptops without protective casing, leaving in car overnight, etc.)
- Storing your own personal data on a school device.
- Storing school information on a device that is not subject to back up routines.

We define the following as **forbidden** use of electronic devices:

- Loading any files containing pornographic, obscene or offensive content onto the schools systems or devices.
- Storing personal material which is subject to copyright, without the correct purchase and licensing (e.g- pictures, music, games, videos and software that have not been purchased through the formal channels)
- Deliberate, reckless or negligent introduction of a virus or malware into the schools ICT systems. Installation and/or use of software with remote control capabilities without the Headteacher's consent.
- Leaving devices with sensitive data on them unsecured overnight: (e.g. laptops and tablets not hidden and locked away. not shutting down PCs before leaving)
- Leaving any devices that store personal data logged in and unlocked whilst the device is unattended.
- Removing data from the school, on a device or though cloud storage, that is not sufficiently encrypted (e.g. removing a laptop that has not been encrypted, using Pen sticks/DVD/CDs that are not encrypted, uploading sensitive data to OneDrive/Dropbox)
- Loading any unauthorised software onto devices (i.e. any software that has not been purchased through the formal process, including software

- from websites, whether freeware or commercially sold)
- Storing information relating to pupils or staff members on a personal device.
- Not disposing of or storing paper documents containing personally identifiable or sensitive information in a safe, confidential way.
- Attempting to access any computer system that you have not been given explicit permission to access

WARNING It is important to note that the list above is not all encompassing and any other use that may be a security risk, detrimental to children's wellbeing or highly unprofessional, would be subject to consequences.

Use of User Accounts and Passwords

This section of the policy relates to, but is not exhaustive of the following:

- The St. Gabriel's User Network
- The SIMS network
- School E-mail accounts (e.g. as Office365)
- Assessment accounts (e.g. Target Tracker accounts)
- Curriculum Resource Accounts (e.g. ActiveLearn, PurpleMash, Hamilton Trust, Spelling Shed, Come and See)

We define the following as acceptable use of user accounts and passwords:

- Carrying out your work using our own user accounts, where
- personally assigned.
- Carrying out only business work on all accounts assigned
- (personal or school accounts) .
- Using administrator accounts to carry out duties assigned to you by the Headteacher, as part of your role
- Access to user accounts without the owner's explicit permission. Note: this will only occur when given permission from the Headteacher for a legitimate business need.
- Adherence to the schools policy on safe passwords (see eSafety policy section 4 for full details)

We define the following as unacceptable use of user accounts and passwords:

- Requesting the user account and password that has been assigned to another user.

We define the following as forbidden use of user accounts and passwords:

- Sharing a password associated with any user account assigned to you
- Resetting the password associated with a user account assigned to someone else, without their explicit permission.
- Providing the password for a user account personally assigned to another member of staff.

- Using an account that belongs to another member of staff without permission from the Headteacher.
- Using a session established by another user under their own personal account. Using a privileged user account to access data where there is no specific business to do so.
- Not adhering to the schools policy on safe passwords

WARNING It is important to note that the list above is not all encompassing and any other use that may be a security risk, detrimental to children's wellbeing or highly unprofessional, would be subject to consequences.

Use of Telephones

This policy covers the use of the following devices within the school

- School mobile phones
- School landlines
- Personal mobile phones

It is the Headteacher's responsibility to monitor the use of these within school.

We define the following as acceptable use of telephones:

- Use of the schools phones for normal business use.
- Taking the schools mobile phone when out on visits and trips.
- Staff personal mobile phones and communication devices
- used in the designated area only (staff room)
- Visitor's personal mobile phones and communication devices switched off on entry.

We define the following as unacceptable use of telephones:

- Allowing use of schools landlines and mobiles by unauthorised person/s
- Excessive use of personal phones during work hours, to make calls, access the internet or send messages
- Incurring roaming charges on schools mobile phones.
- Using personal mobile phones whilst on visits, trips and during training courses, unless given permission from the Headteacher.

We define the following as forbidden telephone use:

- Use of the schools phones to make personal calls, except in an emergency where a manager is informed.
- Use of phones in a manner that could bring the school into disrepute
- Sending SMS or MMS messages that contain information that is discriminatory, abusive, racist, pornographic, obscene, illegal, offensive or potentially libellous or defamatory.
- Use of the schools phone to promote any external private business Use of the schools phone to contact any premium rate numbers

- Use or storage of personal mobile phones/communication devices in areas outside of those designated, where children may be present

WARNING It is important to note that the list above is not all encompassing and any other use that may be a security risk, detrimental to children's wellbeing or highly unprofessional, would be subject to consequences.

Use Social Media

This policy covers the use of the following within the school

- Twitter

It is the Headteacher's responsibility along with the E-Safety Coordinator and Computing lead to monitor the use of Twitter in school.
We define the following as acceptable use of Twitter:

- The sharing and showcasing of wonderful things happening at St. Gabriel's Catholic Primary School
- To share important announcements and notices as part of general communication to parents
- If staff have individual, personal accounts it will be up to the individual teacher to decide whether they follow the school account.

We define the following as unacceptable use of Twitter:

- Offensive language or remarks aimed at the school, its staff, parents, governors or others affiliated with the school;
- Unsuitable images or content posted into its feed;
- Unsuitable images or content finding its way from another's account into the
- school feed.
- Images or text that infringe upon copyright;
- Comments that aim to undermine the school, its staff, parents, governors or others affiliated with the school.

We define the following as forbidden use of Twitter:

- In no circumstances should pupils be allowed to follow staff
- To use a child's name when tweeting.

WARNING It is important to note that the list above is not all encompassing and any other use that may be a security risk, detrimental to children's wellbeing or highly unprofessional, would be subject to consequences.

Guidance for Members on the use of ICT equipment.

Why is ICT important in school?

The schools position on acceptable, unacceptable and forbidden use of technologies in school is defined below:

Without the use of the technologies adults in the school would be unable to complete their roles efficiently. They would not be able to communicate effectively with others or deliver what is expected as part of the National Curriculum. As a result, they would be unable to meet some of the requirements set out by Ofsted.

Technologies are part of everyday life and without using these in the school environment children would not leave the school adequately prepared for life in the modern world.

The school is committed to the task of ensuring that children are prepared for life in a digital age, and that systems are in place to support adults in their roles of employment

Shortly after induction, all staff will be given relevant user accounts, telephone numbers and email addresses, together with details on how to access this advice and support. Outside of the provision of equipment and facilities, a range of training for all abilities is available on a school year group and individual basis.

In addition to this children will be allocated user accounts and have their own e-Safety and acceptable use contract in child friendly language. This will outline what is expected and will require both a pupil and parent/carers signature (see appendix 2) Further to this, regular education will take place on how to use these technologies safely and securely as part of the computing curriculum and safeguarding requirements

How can I ensure protect the information that I have access to?

Staff are reminded that, at all times they must adhere to the school's code of Conduct and safeguarding requirements and the Data Protection Act 1998.

What equipment and support is provided?

Equipment provided to individuals varies based on job role within the school. Items that may be provided are listed throughout this policy and school reserves the right to change these items, where a more cost effective or efficient device/service becomes available.

As part of their contract with ABtec Computer Solutions Limited the school offers technical support and maintenance for laptops, tablets, projectors and interactive whiteboards. For training and support in all other technologies and services the school will provide training and support led by either subject coordinators, senior staff members or external agencies.

In the event of unavoidable, accidental failure or damage to equipment: the school will provide a repair or replacement. Where the failure or damage is deemed to have been avoidable or purposeful, the user will be accepted to bear the cost of repair/replacement

What rules apply to my use of ICT?

This ICT usage policy must be adhered to by every individual who uses the school's technologies and systems. **This must have been fully read, understood and this understanding will be acknowledged through signing Appendix 1 of this document. If you do not understand any part of this policy please speak to the Headteacher and Computing Coordinator prior to signing.**

Confidentiality

- **Maintain confidentiality**. Do not leave your device anywhere they are at risk of theft or where unauthorised people may be able to read its contents. If yo take equipment out of the home or office, keep it with you at all times, or lock it away securely and out of sight. Use a password lock for any hand held devices so that when they are idle for a defined period of time, they lock.
- **Follow all instructions given to you** regarding protection of data, particularly sensitive data. Do not use or leave your devices in areas where unauthorised people can view them.
- **Do not let others use your** login. Do not reveal your usernames and passwords to anyone.
- **Do not access other people's files, directories, log in details or data** unless given explicit permission to do so within the realms of legitimate business use.
- **Do not copy or transmit data outside of the school** unless given explicit permission to do so within the realms of legitimate business use.
- **Be sensible sending e-mails and messages** they can be viewed and monitored by others and once they have left the school network they are no longer protected

Use of Electronic Equipment

The school's position on acceptable, unacceptable and forbidden use of electronic equipment is defined at section 2.2 of the policy.

Use of E-mail Services

The school's position on acceptable, unacceptable and forbidden use of email is defined in section 2.2 of this policy. Please adhere to the points made in this section and report any incidents of inappropriate material immediately to the Headteacher.

- **Please manage your email box** within the limits allocated to you. When you are notified that your mailbox is approaching capacity, kindly remove items to create more space.
- Please remember that you can **save emails in personal folders** if you prefer to keep them for reference.
- **Be aware** that emails and data stored on the Council's network and servers, can be viewed if there is a requirement to do this and may be subject to disclosure under the Freedom of Information Act.
- This includes text messages from the school messaging system and school mobiles. Please bear in mind when sending messages by these methods.

How can I get advice about any issues?

Please contact the schools Computing Coordinator or Headteacher and where appropriate the school's designated representative from ABtec Computer Solutions Limited

Section Three

Monitoring

St. Gabriel's Primary School reserves the right to monitor and keep records of any use of its ICT for a number of reasons relevant to the school's services, including but not limited to:

- Ensuring compliance with this policy and other related policies such as the code of conduct, safeguarding and eSafety
- Training and monitoring standards of service
- Identifying whether internal or external communications are relevant to the school's business
- Preventing, investigating or detecting unauthorised or criminal activities through the use of the school's ICT
- Maintaining the effective operation of the school's ICT System
- E mails addressed to you which are received during your absence from work (eg, due to sickness or holiday), may be reviewed by the Headteacher, where there is a legitimate need to do so.

Authorised officers may occasionally need to undertake activities that fall into 'Unacceptable' or 'Forbidden' categories to carry out their daily work (e.g. ABtec may need your log in details when working on your staff laptop) This is acceptable provided that it is done with the full knowledge and agreement of the Headteacher who will be informed of the activities.

The school fully appreciates that users have legitimate expectations that they can keep their personal lives private and that they are also entitled to a degree of privacy whilst in the work environment. However, all users should take note that every person who uses the Council's ICT to send or receive information may have their communications intercepted and logged, even if it is marked as private or personal.

St. Gabriel's Primary School uses both automated and manual monitoring techniques on many of their systems, including

- E-mail recording, logging and filtering
- Call, sms and text logging (including content)
- Anti-virus protection
- Web content and URL logging and filtering
- Anti-hacking and anti-spy ware tools

This level of monitoring is deemed as both appropriate and necessary to ensure that the school is able to continue to use these technologies and services without risking data security or children's safety. Whilst we recognise that the vast majority of users respect acceptable use we are required to safeguard all parties involved and to support confidentiality, only designated staff members will be allowed to monitor content in certain areas. Information from monitoring will only be passed to others when it is deemed to be

a breach of policy, when it is required to comply with court orders or needed to facilitate criminal investigation.

The school is responsible for all data held on the technologies and systems it supplies and as a result it retains the right to monitor the content of such data for legal compliance.

Section Four

Glossary of Terms

A number of terms are used throughout this Acceptable Use Policy that may need further definition, Terms are listed below to further aid understanding.

ICT - refers to system/applications internet, e mail, mobile devices including telephones and tablets, landlines, cameras and personal computers and servers.

Offensive - It is not possible to provide an exhaustive list of 'offensive' material the following identifies examples of the type of material that does fall within the definition of offensive in accordance with this policy
Material that is defamatory, racist or discriminatory on grounds of religion, disability, gender or sexual orientation, or alternatively which is designed to harass, victimise or bully, cause pain or distress to individuals.

Obscene - Literal definitions of obscene' describes material that is "offensive or disgusting by accepted standards of morality and decency", material that is designed to deprave or corrupt the audience. For the purpose of this document, any material that will cause extreme offence to a school employee, parent pupil, business partner or visitor will be considered obscene.

Compressed Files - These are ordinary files that have been modified to decrease the space they take up. They are extremely large files when uncompressed and can take up large amounts of space on devices and servers. They are usually saved with an ending of zip as their extension

Executable File - This is a file that contains a program that is used to install and run programs on devices. It usually has a file name extension of bat..com, or exe at the end.

Limited Use - This is not prescribed and varies according to the amount of time which the employee has spent not undertaking their legitimate work. An example would be 1 occasion per week, for a period of up to 5 minutes each time and where it is of no detriment to the school pupils.

Excessive Use - This is not prescribed and varies according to the amount of time which the employee has spent not undertaking their legitimate work. An example would be in excess of 3 times per week, for periods of more than 5 minutes each
time

Session - A session in this document relates to a period of time spent on a connected device where an interaction can take place unhindered. Sessions are normally defined by a

log on and log off action, or unlocking and locking a Workstation using ctrl/alt/delete keys

Adequate protection or encryption - confidential, sensitive or personal information must be protected or encrypted using complex passwords of at least 8 characters of which at least 1 must be of numeric value.

Other policies which may contain relevant information pertaining to this policy include:

- The Safeguarding Policy
- The Staff Code of Conduct
- The E-Safety policy

Appendix 1: Staff Signatures

I can confirm that I have thoroughly read and understood this policy and that I am fully aware of my roles and responsibilities in adhering to it.

Name	Role	Signature

Appendix 2: Children's Acceptable Use Policy

Key Stage One Contract

At St. Gabriel's I get to use lots of different equipment.

I am allowed to:

- Use things with an adult.
- Have my own username and passwords for programs.
- Tell a teacher is something upsets me.

I am not allowed to:

- Use things without an adult.
- Tell other people my username and passwords.
- Use other people's username and passwords.

To keep me safe my school:

- May stop me looking at some pictures, videos and websites
- Can see what I look at or search on my computer

I follow these rules:

- People might be upset
- I won't be allowed to use the equipment
- I won't earn my full playtime
- Mrs Williams might have to speak to me
- Mrs Williams might have to speak to my parents.

Pupil: My teacher has read the rules to me and I understand them.

Signed: _____

Parent:

I _____ have read and understood these rules and understand my child's and the school's responsibilities for the use of ICT equipment and services.

Signed: _____

Key Stage Two Contract

As a pupil at St. Gabriel's I get to use equipment like laptops, iPads, digital sciences equipment and lots of cool technologies. I also get to use the Internet

I am allowed to:

- Use the equipment carefully with an adult
- Have and use my own username for the laptops, Purple Mash, Spelling Shed and Active Learn.
- Create safe passwords for the laptops, Purple Mash, Spelling Shed and Active Learn,
- Use the internet to search when an adult is with me.
- Use websites given to me by a teacher to help me learn.
- Tell a teacher if I see anything on the internet that might upset someone
- Hand my electronic devices into the office for safe keeping if I accidentally bring them into school.

I am not allowed to:

- Use the equipment when there are no adults
- Tell people my username and passwords.
- Use other people's username and passwords.
- Use the internet to search when there are no adults.
- Go on different websites to those my teacher has said.
- Bring any electronic devices into school including mobile phones

Key Stage Two Contract
-+

To keep me safe at school :

- Has special software that blocks adverts and upsetting websites.
- Has special software that can see what people have typed into the computers.
- Has special software that can see what people have looked at on the internet.
- Has special software that prevents Viruses and malware stealing my information or ruining our school equipment.
- Has special software so I can only look at my stuff on the computer.

If I do not follow these rules:

- I might get upset.
- I might upset someone else
- I might lose my work.
- I might get in trouble for something someone else did on my account
- I might be told that I cannot use the equipment for a bit.
- I might not earn my full reward points and break time.
- Mrs Williams might have to speak to me
- Mrs Williams might have to speak to my parents.

Pupil:

I _____ have read these rules with my teacher and I understand what I need to do to use ICT equipment.

Signed _____

Parent:

I _____ have read and understood these rules and understand my child and the school's responsibilities for the use of ICT equipment and services.

Signed _____