

SS Peter and Paul Catholic Primary School



Equipment Acceptable & Responsible Use Agreement

Date updated: March 2022

Review Date: March 2024

Please read this Acceptable & Responsible Use Agreement that has been shared with you via email. If you require a paper copy, please ask the school office, who will provide this for you.

Once you have read and replied to this email confirming you agree to the terms and conditions of this agreement, please discuss this with your child.

Please contact us if you have any questions.

At Ss Peter and Paul Catholic Primary we are committed to using educational technology to improve further the learning experiences and achievements of all of our pupils. Technology provides us with opportunities to inspire and motivate our young people to achieve their full potential and engage them fully in their learning. We believe that the use of technology will enhance everyday learning and teaching and in particular will:

- Raise educational attainment
- Create a pupil centred curriculum, which will provide engaging pupil centered lessons
- Enable pupils access to the most up to date educational resources
- Raise levels of engagement, motivation and interaction
- Improve facilitation of different learning styles
- Promote remote & independent learning
- Develop children's confidence levels
- We recognise and encourage the use of technology home to promote remote learning.

This policy applies to all pupil users wherever they are physically located - either within the school or at home. It is intended to complement the school's wider e-Safety, Safeguarding and Behaviour Policies.

Due to the changeable nature of technology, this policy will be reviewed regularly and as such, the school reserves the right to amend any sections or wording at any time.

The following details define the proper use of the device both in and out of school hours.

Device Loan

The school will retain complete ownership of the device.

If a child leaves the school the device must be returned to the school immediately. In certain circumstances, the device could be transferred to the new school (this must be agreed with the school prior to the child leaving).

Pupils should not loan or share the device with other people.

Passwords and Logins

Children should take reasonable measures to secure access to the device by using a password.

Children are not allowed to remove the password from the device or share this password with anyone else except their parents/carers, and a designated member of staff (this will be requested during the initial set-up process).

Photographs and Images (still & moving)

Photographs/Images stored on the device must be appropriate; the school reserves the right to randomly check any device for unsuitable content. Recording, photographing or filming of any other children or school staff is strictly forbidden, unless specifically permitted by the class teacher. No images or video material taken in school may be uploaded from any device to social networking sites.

Photos and videos should be deleted regularly by pupils for safeguarding and data storage reasons.

Software and Applications

Children will not be given the ability to install or delete any applications on the device.

If this agreement is breached in any way, school may apply additional restrictions to the device to safeguard your child.

Applications provided by the school for educational use, remain the property of school at all times.

The School will provide software on the device. The Software originally installed by the school must remain on the device in a usable condition and be easily accessible at all times. From time to time, the school may add or modify software applications. The school's remote management system monitors all devices and may be flagged if inappropriate material is accessed at home. Periodic checks of the device will be made to ensure that students have not removed required software or downloaded applications which are deemed inappropriate (either by their age-restriction or content).

Internet Access

The school will monitor and filter internet access.

Children may only access the internet through secure access provided by the school. Pupils are not permitted to access the internet via their own mobile connection 3G/4G functionality (or otherwise/ personal hotspotting), as this is unmonitored and unfiltered access.

Ss Peter and Paul Catholic Primary will not accept responsibility for personal data that children store on their device. We assure you that we comply with the principles of the Data Protection Act; we will process any data lawfully and fairly and any data held will be kept secure and safe within our managed system.

The school uses Google Apps for Education. Virtual lessons and contact with teaching staff will only be made using this platform.

Games, video conferencing and Social Media

Children are permitted to access gaming sites at home providing they:

- Do not violate any terms of this agreement
- Are age-appropriate
- Do not contain social networking of any kind (these sites are not permitted)
- Do not affect the amount of storage needed in order to run applications needed for educational purposes.

The device can be used to join a video conference with the class teacher via Google Meet. These sessions will be set up by the school and monitored and controlled by them. Children are not permitted to create or continue in their own video conference sessions.

Social media of any kind is not permitted on the device. Filtering of internet access does not permit access to social media sites, sites with chat facilities, gambling sites, or other sites that are illegal or inappropriate for children.

Inspection of devices

Pupils may be selected at random to provide their device for inspection so that the school can ensure they comply with the safeguarding measures outlined in this policy.

Procedure for reloading software

If technical difficulties occur, or inappropriate software/applications/content is discovered, the device will be restored to the default factory settings and additional restrictions applied to safeguard your child. The school does not accept responsibility for the loss of any software or data deleted due to a re-format and re-image.

Regular Software Updates

Upgrade versions of licensed Software/Applications are available from time to time. These will be managed by the school.

Device identification

The device will be labelled in the manner specified by the School. Equipment can be identified in the following ways:

- Serial Number or asset number
- The device will be named in accordance with school's procedures, and this must not be changed
- The school may enforce the enabling of Location Services on iPads in order to use the 'Find My iPad' app. This will be used as a security measure to minimise loss or theft

Device Security

All equipment will be managed centrally by the school. This management system allows the school to send out applications, reset passcodes, update software and set restrictions. This management system must never be removed from the device.

The equipment is installed with forensic software that monitors activity on the device. All keystrokes are monitored and a report generated detailing any activity that is suspicious or illegal or inappropriate. The report is sent to the designated member of staff at the school, usually the head teacher, who will then decide on what action to take.

Parent/Carer Responsibilities

Parents/carers are expected to talk to their children about the values and standards that they should follow on the use of the Internet, just as they do on the use of all media information sources such as television, telephones, movies, radio, iBooks etc.

Parents/carers are expected to:

- ensure that their child keeps their device safe and uses them in accordance with the school procedures outlined above
- ensure that their child uses their device in accordance with school policies
- allow their son/daughter to use their device at home to assist them with homework and wider learning, and to monitor and oversee use within the home setting
- to ensure their child's online safety by supporting the guidance provided by the school
- make every effort to ensure that the device does not incur damage, loss or theft.

Children are expected to:

- Use the equipment in a responsible and ethical manner
- Obey general school rules concerning behaviour and communication that apply to technology use
- Use all computer resources in an appropriate manner so as to not damage school equipment
- Turn off and secure their device (with their passcode) after they are finished working to protect their work and information
- Report any inappropriate content or abusive language to a member of school staff immediately
- Make no changes to the device profile (this does not include changes to accessibility settings to support learning)

Activities specifically prohibited

In addition to the school's wider policies on the acceptable use of the Internet, children are not permitted to:

- Illegally install or transmit copyrighted materials
- Loan their device to anyone else, unless specifically asked by a teacher
- Change device settings (exceptions include personal settings such as font size, brightness, etc.)
- Download vault or ghost applications to keep content hidden
- Download prohibited applications or those which are not age-appropriate
- Use or access another student's device without specific instruction from a teacher
- Attempt to modify, upgrade or repair equipment issued under this policy
- Send or display offensive or inappropriate messages or material
- Use obscene language or content
- Be used for the purpose of bullying or excluding another child

- Cause deliberate damage to operating systems, devices, or other technology-related resources
- Use other people's passwords
- Download illegal content or material that is suspicious/inappropriate
- Upload any photo or video content taken to any social networking sites
- Use bluetooth or airdrop without permission from a member of school staff
- Use video streaming or messaging outside of an educational session

Legal Proprietary

All pupils and parents/carers should comply with trademark and copyright laws and all license agreements. Ignorance of the law is not immunity. If any parties are unsure, they should seek advice. Use or possession of hacking software is strictly prohibited. Violation of the law may result in criminal prosecution or disciplinary action.

Inappropriate Use

Any pupil who persistently refuses to cooperate, or violates any aspect of school policy, may face other disciplinary action deemed appropriate in keeping with the school's Behaviour Policy. Violations may result in disciplinary action up to and including suspension/expulsion for pupils. When applicable, law enforcement agencies may be involved.

Pupil equipment checks can be conducted by any member of staff at any time during the school day. These can be random and unannounced spot checks.