Signed……………………………..

Date………………………………..

Review…………………………….

Woodford Valley C of E Primary Academy
Acceptable Use Agreement for Academy Staff

This school is committed to creating the ethos in which children can grow towards Christian life, learning and love.

'And now I give you a new commandment: love one another. As I have loved you, so you must love one another. If you have love for one another, then everyone will know that you are my disciples."
John 13 34-35

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 access to the internet and digital technologies 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 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 technology in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for 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 systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that pupils receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.
For my professional and personal safety:
• I understand that the school will monitor my use of the school digital technology and communications systems.

•   All staff to complete statutory annual cyber security training and any other online security/safeguarding training identified by the school

- I will share with the senior management team any IT professional development I may require through the performance management system

• I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, VLE etc.) out of school, and to the transfer of personal data (digital or paper based) out of school.

• I understand that the school digital technology systems are primarily intended for educational use and that I will not use the systems for personal or recreational use.

I will only use my personal device during official breaks in the staff room or in a room where children are not visible.

• 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 understand that I should not write down or store a password where it is possible that someone may steal it.

• I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

- I will not leave laptops/desktops open with sensitive/confidential information displayed on screens

I will be professional in my communications and actions when using trust 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 (e.g. 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 social networking sites in school in accordance with the school's policies.

• I will only communicate with 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, including sharing information about the school and staff.

- I will report misuse of social media by the school community where the school reputation maybe damaged

The trust has the responsibility to provide safe and secure access to technologies and ensure the smooth running of each school:

• When I use my mobile devices in school or to access my school/ trust email account outside of school settings, I will follow the rules set out in this agreement and policy, in the same way as if I was using school equipment.

• I will only use my mobile phone in line with the requirements of the policy and will ensure that any pop-up notifications are removed from my smart watch.

• I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes). Should I inadvertently click on an attachment that looks suspicious I will follow the instructions for– Cyber Security Concern or Personal Data Breach.

• 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, terrorist or extremist 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 be responsible for replacing damaged equipment where damage has occurred due to misuse/inappropriate use.
- I will return all school equipment at the end of any term of employment.

I will only transport, hold, disclose or share personal information about myself or others, as outlined in the trust Data Protection Policy Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based documents containing personal data must be held in lockable storage.

• I understand that the trust 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 online systems in my professional capacity:

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 the school:

• I understand that this acceptable use policy applies not only to my work and use of the school's digital technology equipment in school settings, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the trust/ school

• I understand that if I fail to comply with this acceptable use agreement, I could be subject to disciplinary action. This could include a warning, a suspension or referral to the Head teacher or Trustees as part of a Disciplinary process 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 digital technology 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/ Student/Contractor Name:
Signed:
Date:

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not access online content (including apps, games, sites) to make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	**Any illegal activity for example:** • Child sexual abuse imagery* • Child sexual abuse/exploitation/grooming • Terrorism • Encouraging or assisting suicide • Offences relating to sexual images i.e., revenge and extreme pornography • Incitement to and threats of violence • Hate crime • Public order offences - harassment and stalking • Drug-related offences • Weapons / firearms offences					X

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
	• Fraud and financial crime including money laundering **N.B. Schools should refer to guidance about dealing with self-generated images/sexting – UKSIC Responding to and managing sexting incidents and UKCIS – Sexting in schools and colleges**					
Users shall not undertake activities that might be classed as cyber-crime under the Computer Misuse Act (1990)	• Using another individual's username or ID and password to access data, a program, or parts of a system that the user is not authorised to access (even if the initial access is authorised) • Gaining unauthorised access to school networks, data and files, through the use of computers/devices • Creating or propagating computer viruses or other harmful files • Revealing or publicising confidential or proprietary information (e.g., financial / personal information, databases, computer / network access codes and passwords) • Disable/Impair/Disrupt network functionality through the use of computers/devices • Using penetration testing equipment (without relevant permission) **N.B. Schools will need to decide whether these should be dealt with internally or by the police. Serious or repeat offences should be reported to the police. The National Crime Agency has a remit to prevent pupils becoming involved in cyber-crime and harness their activity in positive ways– further information can be found here**					X
Users shall not undertake activities that are not illegal but are classed as unacceptable in school policies:	Accessing inappropriate material/activities online in a school setting including pornography, gambling, drugs. (Informed by the school's filtering practices and/or AUAs)				X	
	Promotion of any kind of discrimination				X	
	Using school systems to run a private business				X	
	Using systems, applications, websites or other mechanisms that bypass the filtering/monitoring or other safeguards employed by the school				X	
	Infringing copyright				X	
	Unfair usage (downloading/uploading large files that hinders others in their use of the internet)				X	
	Any other information which may be offensive to others or breaches the integrity of the ethos of the school or brings the school into disrepute				X	

Consideration should be given for the following activities when undertaken for non-educational purposes: **Individual schools may wish to add further activities to this list.**	Staff and other adults					Pupils			
	Not allowed	Allowed	Allowed at certain times	Allowed for selected staff	Allowed during official breaks on own device	Not allowed	Allowed	Allowed at certain times, to be specified by class teacher	Allowed with staff permission
Online gaming					X	X			
Online shopping/commerce for personal use					X	X			
Online shopping for work purposes		X				N/A			
External File Sharing to appropriate people		X				X			
Social Media for school/ trust purposes		X				X			
Social Media					X	X			
Messaging/ Chat for work purposes on Teams		X				X			
Messaging/ Chat for work purposes via Text, WhatsApp or similar			X			X			
Entertainment streaming e.g. Netflix, Disney + in classrooms at appropriate times		**X**				X			
Use of video broadcasting, e.g. YouTube, Twitch, TikTok for work purposes		X				X			
	Staff and other adults					Pupils			

Consideration should be given for the following activities when undertaken for non-educational purposes: **Individual schools may wish to add further activities to this list.**	Not allowed	Allowed	Allowed at certain times	Allowed for selected staff	Allowed during official breaks on own device	Not allowed	Allowed	Allowed at certain times, to be specified by class teacher	Allowed with staff permission
Mobile phones may be brought to school		X				**X**			
Smart watches may be brought into school		X but pop up notifications must be removed				X			
Use of mobile phones for learning at school		X				X			
Use of mobile phones in social time at school					X	X			
Taking photos on mobile phones/cameras		X				X			
Use of other personal devices, e.g. tablets, gaming devices					X	X			
Use of school email for personal e-mails	X					X			