<div align="center">

West End Primary School

Acceptable Use Policy Agreement for Staff and Volunteers

</div>

This policy is intended to be read and agreed in conjunction with the following policies:
- E-Safety
- Child Protection
- Anti-bullying
- Anti-racism
- Data protection

School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

• that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

• that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

• that staff are protected from potential risk in their use of ICT in their everyday work.

The school will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for pupils' learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that pupils receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

For my professional and personal safety:
• I understand that the school will monitor my use of the ICT systems, email and other digital communications.

• I understand that the rules set out in this agreement also apply to use of school ICT systems (eg laptops, email, VLE etc) out of school, and to the transfer of personal data (digital or paper based) out of school (as detailed in the E-safety policy – table appended)

1

- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school. (as detailed in the E-safety policy – table appended)
- 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 be professional in my communications and actions when using school ICT systems:
- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (eg on the school website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use chat and social networking sites in school in accordance with the school's policies. (detailed in the E-safety policy – table appended)
- I will only communicate with pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner. (further advice is included in the E-safety policy)
- I will ensure that emails containing sensitive or personal identifiable data are removed to a separate folder, once processed, to reduce the risk of unauthorised disclosure.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my mobile devices (PDAs / laptops / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses. (detailed in E-safety policy – table appended)
- I will ensure the security of any school or personal devices in my possession when out of the school building, making sure that they are physically secure and that the use of my school e-mail systems cannot be accessed by any other person by keeping log-ins, passwords and login matrices private and secure.
- I will not use personal email addresses on the school / academy ICT systems.
- 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)
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.

- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies. (further advice is included in the E-safety policy)
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Data Protection Policy. Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.
- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:
- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the school:
- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action, as detailed in the E-safety policy – table appended.

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name

Signed

Date

Implementation and review process

This policy was reviewed as part of the E-safety policy agreed by the Strategic Direction Committee of the Governing Body and implemented in February 2021

AUP agreement statements were created as an Appendix of the E-safety Policy and will be reviewed with the policy on a bi-annual basis or as required by changes in safeguarding responsibilities.

Date of next review: February 2022

Acceptable Use tables

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	*							*
Use of mobile phones in lessons				*				*
Use of mobile phones in social time		*						*
Bluetooth enabled				*				*
Taking photos on mobile phones or other camera devices		*						*
Use of hand held devices eg PDAs, PSPs		*						*
Use of personal email addresses in school, or on school network				*				*
Use of school email for personal emails				*				*
Use of chat rooms / facilities				*				*
Use of instant messaging				*				*
Use of social networking sites				*				*
Use of blogs		*					*	

	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal

User Actions

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					*
	promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation					*
	adult material that potentially breaches the Obscene Publications Act in the UK					*
	criminally racist material in UK					*
	pornography				*	
	promotion of any kind of discrimination				*	
	promotion of racial or religious hatred				*	
	threatening behaviour, including promotion of physical violence or mental harm				*	
	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				*	
Using school systems to run a private business					*	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by NCC and the school					*	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions					*	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					*	
Creating or propagating computer viruses or other harmful files					*	
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					*	
On-line gaming (educational)			*			
On-line gaming (non educational)			*			
On-line gambling					*	
On-line shopping / commerce			*			
File sharing					*	
Use of social networking sites					*	
Use of video broadcasting eg Youtube			*			

Responding to incidents of misuse

Actions and Sanctions

Incidents:	Refer to line managerr	Refer to Head teacher	RRefer to Local Authority / HR	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).		*	*	*				
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email	*	*			*	*		
Unauthorised downloading or uploading of files	*	*			*	*		
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	*	*			*	*		*
Careless use of personal data eg holding or transferring data in an insecure manner	*	*			*	*		
Deliberate actions to breach data protection or network security rules	*	*	*		*	*		*
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	*	*	*		*	*		*
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	*	*	*			*		*
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	*	*	*		*	*	*	*
Actions which could compromise the staff member's professional standing	*	*				*		
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	*	*	*			*		*
Using proxy sites or other means to subvert the school's filtering system	*	*			*	*		*
Accidentally accessing offensive or pornographic material and failing to report the incident	*	*	*		*	*		*
Deliberately accessing or trying to access offensive or pornographic material	*	*	*		*	*	*	*
Breaching copyright or licensing regulations	*	*	*		*	*		*
Continued infringements of the above, following previous warnings or sanctions	*	*	*		*	*	*	*