Winnington Park Primary School and Nursery

Acceptable Use of Communications Policy

Completed by: Kay Ikin

Updated: Autumn 2023

Review date: Autumn 2024

Introduction and Aims

The use of electronic equipment, technology and information carries certain risks which can affect WPPS&N/CWAC in terms of legal liability, reputation and business effectiveness. Use of ICT systems must be in an ethical, professional and lawful manner. In addition, electronic communications within Government Agencies are subject to increasingly stringent standards and it is vital that as a school we comply with standards such as the Government Connect Code of Connection in order to maintain vital services. The purpose of this policy is to establish the way ICT facilities and resources provided to Staff in order to perform their duties must be used.

Scope

The scope of this policy extends to all departments, employees, councillors, contractors, vendors and partner agencies who use/access ICT facilities provided or managed by WPPS&N/CWAC, either directly or on their behalf by contractors and service providers.

This policy should also be read in conjunction with the Online Safety Policy, Mobile Phone Policy, Safeguarding Children Policy, Anti-Bullying Policy and Guidance on the Use of Photographic Images and Videos of Children in Schools.

Communication:

The policy will be communicated to staff/pupils/community in the following ways:

- Policy to be posted on the school website
- Policy to be part of school induction pack for new staff
- Acceptable use agreements discussed with pupils at the start of each academic year
- Acceptable use agreements to be issued to all employees and permanently contracted staff, usually on entry to the school and then annually
- Acceptable use agreements to be held in personnel files

Standards of Conduct

General Use of ICT Systems

Any information created or held on ICT systems will ***not*** be considered personal by default. It may, however, be deemed to be personal when reviewed by the CWAC Information Assurance Team when authorised to identify if it is of a personal private nature. This includes email and internet communications.

Limited personal use of ICT systems is allowed provided it is in the individual's own time and the following conditions are met:-

- The sending and receipt of personal email messages is not excessive and does not interfere with work commitments of the sender.
- The email messages do not constitute misuse of email as detailed in this policy.
- The emails do not relate to any private business activities of the user or his or her relatives, friends or associates.
- WPPS&N/CWAC name used in an email could in no way be construed as adding weight or influencing the person or organisation receiving the email.
- School email accounts/addresses are not to be used for sending personal emails.

When using ICT Systems you must make sure that you communicate in a way that supports the relevant WPPS&N/CWAC policies and procedures that are specific to your role as well as corporately adopted, including those on equalities. You should therefore make sure that you **do not** send/upload/post information on-line which:

- Damages the organisation's reputation or undermines public confidence in WPPS&N/CWAC, its staff, councillors, role or services;
- Supports Political activity (other than any required in your role);
- Includes any libellous, offensive or defamatory material about any individual, firm, body or organisation; or
- Could be deemed to harass, bully or stalk another person.

WPPS&N/CWAC does not accept any liability for any loss or damage to any items or monies arising from use by any staff or anyone else undertaking personal financial transactions or related order issues over the Internet on any computer.

It is recognised that staff at WPPS&N may on a rare occasion need to use personal electronic equipment and technology for work - the standards of conduct in this policy will apply to your personal equipment when you are using it for work purposes.

If you make an electronic comment on the internet (blogs, social media, twitter etc.) on a personal basis you must be aware that, as an employee of the WPPS&N/CWAC, you are expected to comply with the standards of conduct and behaviour in this and other related policies for example: the Employee Code of Conduct, the Disciplinary Code.

Staff indicating their affiliation with the WPPS&N/CWAC, e.g. via an email address or other identifier, in bulletin boards, special interest groups, forums or other public offerings, in the course of their business must clearly indicate that the opinions expressed are not necessarily those of WPPS&N/CWAC. Staff should be aware that such a statement does not exempt them from ensuring those views do not reflect negatively on WPPS&N/CWAC.

You must not claim to represent the views of WPPS&N/CWAC unless you have permission to do so as part of your job. Similarly, you must not try and pass off your own comments or views as being from someone else by, for example, falsifying your email address or user name or using someone else's.

Do not send (or forward) email containing derogatory statements, subjective comments likely to cause offence, gossip, hoaxes, joke or chain mail content to other people inside or outside WPPS&N/CWAC. Staff guilty of such activity will be treated with the same possible action as if they were the originator of the content.

The sending of unwanted messages with malicious intent can constitute harassment and would be dealt with as a disciplinary matter.

You must not use social media, the internet, intranet, media, or social media sites to make complaints about your employment, even if areas on these sites are considered 'private'. If you want to make a complaint about any aspect of your employment with WPPS&N/CWAC

you must use the appropriate employment procedure (e.g. Grievance, Fair Treatment at Work, Public Interest Disclosure/Whistleblowing).

Data which involves images of people is covered by strict rules which prevent the use of sensitive data on children and vulnerable adults. You should therefore check any available guidance relating to your job and work area before using this type of data.

You must not post images whose copyright you are not aware. Staff should not assume that because an image is available online it is copyright free and can be used without attribution or payment.

You must make sure that any data stored and/or processed using WPPS&N/CWAC ICT systems complies with the laws on data protection and copyright, is shared only with the intended recipient(s) and only when permission has been given or the information is already widely in the public domain.

The Data Protection Act (1998) requires controls to be put in place to prevent unauthorised access to personal data. This statutory requirement strengthens the need for a high level of appropriate access controls to be developed and implemented.

You must not email, upload or post confidential or sensitive data relating to individuals, partner organisations or any aspect of WPPS&N/CWAC business on the internet or other public service (i.e. DropBox,) without permission from your manager or the owner of the data (see GDPR policies).
When sending email consider if the full email thread is required, ensure that you remove any unnecessary information from the email chain before forwarding on to others.

When emailing multiple recipients together, think about your target audience and consider if there is a need to separate your message. When emailing to groups of external email address the Blind Copy (Bcc) function should be used.

You must maintain security of information by, for example, locking your monitor when leaving your desk regardless of the length of time and by logging off if you will not be using the system for a longer period.

You should not leave any mobile equipment unattended unless it is absolutely necessary and if you do so you must ensure that it is secure and protected from risk of theft or use by others. Staff should not leave mobile equipment unattended on their desk for any length of period and should secure them in a drawer.

You must keep your passwords confidential (don't share them with anyone else) and comply with password security arrangements. This school makes it clear that staff and pupils must always keep their password private, must not share it with others and must not leave it where others can find it. All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password private. We require staff to use strong passwords including capital letters and symbols.

Advised requirements for secure passwords are:

- At least eight characters - Contain characters from three of the four categories: uppercase; lowercase; 0 through to 9; or special characters (*&^%$£"! etc.).
- Are more complex than a single dictionary word (such passwords are easier for hackers to crack).
- Do not contain two of the same characters consecutively.
- Never reveal or share your passwords to anyone and
- Never use the 'remember password' function.
- Never write your passwords down or store them where they are open to theft.
- Never store your passwords in a computer system without encryption.
- Do not use any part of your username within the password.
- Do not use the same password to access different Council systems.
- Do not use the same password for systems inside and outside of work.

You should not try to use or access any part of the WPPS&N/CWAC ICT systems, data or networks which you do not have permission to access or deliberately do anything which would disrupt or damage them in any way.

All organisation or personal data stored on removable media must be **encrypted** including USB sticks. Encrypted and password protected USB memory sticks are provided to all members of staff in need of storing data related for their work purposes. These will be signed for on receipt and must be returned at the termination of employment.

You must not download or install any software, hardware or other devices to WPPS&N/CWAC ICT systems or equipment unless you have relevant authorisation to do so. All installed software must have the appropriate licenses and must be used in accordance with licence agreements.

If you manage or maintain a system it's important to prevent unauthorised access and to ensure that you maintain the confidentiality and integrity of any information, you should:-

- Consider if authorisation is required from the data owner before granting, modifying or changing access to systems or account permissions.
- Ensure that you only give access based on business need. This should be regularly reviewed and access revoked if appropriate.
- Ensure you follow any procedures that are in place to control the allocation and revoking of access rights.

When sending, transferring, taking information offsite or sharing any data you must ensure that you follow WPPS&N/CWAC data sharing process and policies. Appropriate safeguards and controls (e.g. Encryption) must be used.

In conjunction with your position or work related responsibilities you must be aware of any legislation or mandated controls with which WPPS&N/CWAC or its partner organisations must comply with, these may include but are not limited to:

o Data Protection Act (DPA)1998

o Freedom of Information Act (FOIA)2000
o Regulations on the Reuse of Public Sector Information (RPSI) 2005
o Regulation of Investigatory Powers Act (RIPA) 2000
o Computer Misuse Act 1990
o Electronic Communications Act 2000
o Police and Criminal Evidence Act
o Copyright, Design and Patents Act 1988
o Safeguarding of Organisational Records
o Protection from Harassment Act 1997
o Sexual Offences Act 2003
o Defamation Act 1996
o PCI compliance
o PSN Code of connection

It is a criminal offence to use a mobile device whilst driving and a conviction will attract a fixed penalty and a license endorsement. If, in connection with your employment, you are caught driving while using a mobile phone or other device you may be subject to disciplinary action and will be responsible for the payment of any fines/penalties imposed on you. Although hands free device are allowed, use should be kept to a minimum to ensure you are not distracted whist driving.

Personal Use of ICT Systems and School emails

Personal use of WPPS&N/CWAC ICT systems will be permitted on a limited basis, subject to the standards of conduct outlined in this policy. WPPS&N/CWAC reserves the right to restrict personal use of its ICT systems. See above.

Personal use of School Mobile Phones and School Telephones

Read the guidance and requirements in the WPPS&N Mobile Phone Policy about personal mobile phones

It is accepted that you may occasionally need to make an important personal call or to send an important personal email during the school day but these should be kept to a minimum. Personal calls/emails/texts must, be conducted in your own time. (**Note:** This also applies to

personal calls/emails/texts using your own personal equipment during working time). If an urgent communication is required, SLT must be informed so an arrangement can be made. The message must not be taken in the presence of children.

Personal Calls/Text Messages on School telephones: WPPS&N/CWAC reserves the right to charge for personal use of any other ICT systems provided for business use.

Personal Use of the Internet

In addition to all other guidance and requirements in this policy

- Any personal use of ICT systems must not expose security controls, systems or data to risk. You must not:
- Allow non-employees (including family members) to use ICT equipment (including mobile devices, phones and tablets); or
- Attach any personal equipment to ICT systems without the approval of the Information CWAC Assurance and Security Team or Network Technician.
- Store any business critical, personal or sensitive personal information in locations or systems that have not been approved.

You must not knowingly access or try to access inappropriate internet sites, materials or downloads. This includes pornographic, illegal or other sites which would breach the Employee Code of Conduct, Disciplinary Code or equality standards and covers all WPPS&N/CWAC ICT Systems or personal equipment when it is used for work purposes or in work time.

Use of Social Media

Acceptable use of social media includes:

- Being aware at all times that, while contributing to the organisation's social media activities, you are representing WPPS&N/CWAC. Staff who use social media as part of their job must adhere to the principles as set out in the Social Media Responsible Conduct Policy.

- When using social media sites you must not publish or post any information that you have received or have access to as a result of your employment unless you have been given permission to do so as this is confidential to your work.
- You must not use social media sites in any way that may undermine public confidence in the WPPS&N/CWAC or your role within WPPS&N/CWAC, bring the organisation into disrepute, or would be discriminatory or defamatory e.g. publish or post any information including comments, jokes, illegal or prohibited images or other materials which would put WPPS&N/CWAC at risk of legal action.
- You should avoid informal personal contact with service users you work with directly or indirectly, or their carers, through social media sites (e.g. do not add them as a 'friend', 'follow' them or link with them), or using your own personal electronic equipment (e.g. email, text, calls).
- You must not use social media to harass, bully, stalk or behave in any other way that could damage your working relationships with your colleagues, members of the public or elected members.
- Be aware that personal use of social media, while not acting on behalf of WPPS&N/CWAC, could potentially damage the organisation if an individual is recognised as being an employee. Any communications that employees make in a personal capacity through social media must therefore adhere to the principles as set out in this policy.
- Whilst on school premises employees are allowed limited access to social media websites from WPPS&N/CWAC computers/devices or using their own equipment, in their own time and in accordance with this guidance and requirements within this policy and other associated policies.

Monitoring

WPPS&N/CWAC records the use of its systems to measure system security, performance, whether employees are meeting the standards of conduct in this policy and for the prevention and detection of crime. This is covered in the CWAC Monitoring and Investigation Policy. The Local Authority logs all staff internet, Lync and email activity, and reserves the right to access, retrieve and delete:

- all email including in draft form, sent or received;
- all private and shared directories;

- all use of intra/internet and other communication techniques using organisational ICT systems e.g. Twitter, blogs etc; and
- all software on computer equipment.

Use of the telephone, fax systems and mobile telephones may also be logged and may be in some cases be recorded.

Failure to follow the standards of conduct

If you fail to follow the standards of conduct set out in this policy, use of ICT systems may be withdrawn from you and/or disciplinary action taken against you, up to and including dismissal.

Retention of Data

As a school we ensure that we comply with the Data Protection Act 1998 requirements. Staff are made aware that failure to do so could result in enforcement action from the ICO. Privacy notices are published to staff at the start of each year explaining how and why and what data is collected, stored, for how long it is retained and why it is collected. Please read associated policies and guidance documents on how WPPS&N adheres to GDPR guidelines.

Infringement of this Policy

Local Authority guidance and disciplinary procedures will be followed for any member of staff or Governor who does not abide by this and associated policies.

Acceptable ICT Use Agreement: All Staff and Governors

Rules for Responsible Computer and Internet Use

Covers use of all digital technologies in school: i.e. email, Internet, intranet, network resources, learning platform, software, communication tools, equipment and systems.

- I will only use the school's digital technology resources and systems for Professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.
- I will not reveal my password(s) to anyone.
- I will follow 'good practice' advice in the creation and use of my password. If my password is compromised, I will ensure I change it. I will not use anyone else's password if they reveal it to me and will advise them to change it.

- I will not allow unauthorised individuals to access email / Internet / intranet / network, or other school systems, *or any Local Authority (LA) system I have access to*.
- I will ensure all documents, data etc., are printed, saved, accessed and deleted / shredded in accordance with the school's network and data security protocols.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will only use the approved email system(s) for any school business; Microsoft 365
- I will only use the approved *communication systems* with pupils or parents/carers, and only communicate with them on appropriate school business.
- I will not browse, download or send material that is considered offensive or of an extremist nature by the school.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach or equipment failure to the *Computing Lead / Headteacher*
- I will not download any software or resources from the Internet that can compromise the network or might allow me to bypass the filtering and security system or are not adequately licensed.
- I will check copyright and not publish or distribute any work including images, music and videos, that is protected by copyright without seeking the author's permission.
- I will not connect any device (including USB flash drive), to the network that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the school's *recommended anti-virus and other ICT 'defence' systems*.
- I will not use personal digital cameras or camera phones or digital devices for taking, editing and transferring images or videos of pupils or staff and will not store any such images or videos at home.
- I will follow the school's policy on use of mobile phones / devices at school
- I will only use school approved equipment for any storage, editing or transfer of digital images / videos and ensure I only save photographs and videos of children and staff on the *appropriate system or staff-only drive within school*.
- I will use the school's Learning Platform in accordance with school protocols.

- I will ensure that any private social networking sites / blogs etc that I create or actively contribute to are not confused with my professional role.
- I will ensure, where used, I know how to use any social networking sites / tools securely, so as not to compromise my professional role.
- I agree and accept that any computer or laptop loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.
- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I will alert *the School's* child protection officer / appropriate senior member of staff if I feel the behaviour of any child may be a cause for concern.
- I understand it is my duty to support a whole-school safeguarding approach and will report any behaviour of other staff or pupils, which I believe may be inappropriate or concerning in any way, to *senior member of staff / designated Child Protection lead*.
- I understand that all Internet and network traffic / usage can be logged and this information can be made available *to the Head / Safeguarding Lead* on their request.
- I will only use any LA system I have access to in accordance with their policies.
- *Staff that have a teaching role only:* I will embed the school's on-line safety / digital literacy / counter extremism curriculum into my teaching.

User Signature

I agree to abide by all the points above.

I understand that I have a responsibility for my own and others e-safeguarding and I undertake to be a 'safe and responsible digital technologies user'.

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent e-safety policies.

I understand that failure to comply with this agreement could lead to disciplinary action.

Signature ..... Date .....

Full Name ..... (printed)

Job title / Role .....

Authorised Signature (Head Teacher / Deputy)

I approve this user to be set-up on the school systems relevant to their role

Signature ..... Date .....

Full Name (printed)

Example

Acceptable ICT Use Agreement: Parents

Rules for Responsible Computer and Internet Use

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies provide powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

- **The school strongly recommends that children do not use social network sites such as Facebook, Twitter and WhatsApp at home, as these sites carry an age-restriction and pose a risk to children. Social networks have no place in our school and so school staff should not be approached online or invited to join. Children should be encouraged to only use the School's**

Virtual Learning Environment where they can share information, blog and chat in a safe environment.

As the parent / carer of the above students / pupils, I give permission for my son / daughter to have access to the internet and to ICT systems at school.

I know that my son / daughter has signed an Acceptable Use Agreement and has received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.
I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's / daughter's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.

As a parent, I support school policies on ICT and I will ensure that I monitor my child's use of the internet (including social media) outside of school. **I will act as a positive role model to my child, by ensuring that I use social media responsibly.**

Parent/Guardian Name _____

Pupil Name: _____

Signed _____

Date: _____

Online Safety Rules

These Online Safety Rules help to protect pupils and the school by describing acceptable and unacceptable computer use.

- The school owns the computer network and can set rules for its use
- It is a criminal offence to use a computer or network for a purpose not permitted by the school
- Irresponsible use may result in the loss of network or Internet access
- Network access must be made via the user's authorised account and password, which must not be given to any other person
- All network and Internet use must be appropriate to education
- Copyright and intellectual property rights must be respected
- Messages shall be written carefully and politely, particularly as email could be forwarded to unintended readers
- Anonymous messages and chain letters are not permitted
- Users must take care not to reveal personal information through email, personal publishing, blogs or messaging
- The school ICT systems may not be used for private purposes, unless the head teacher has given specific permission
- Use for personal financial gain, gambling, political activity, advertising or illegal purposes is not permitted

Acceptable ICT Use Agreement: Pupils

Rules for Responsible Computer and Internet Use

These rules will keep me safe and help me to be fair to others.

- I will only use the school's computers for schoolwork and homework.
- I will only edit or delete my own files and not look at, or change, other people's files without their permission.
- I will keep my logins and passwords secret.
- I will not bring computer files into school without permission or upload inappropriate material to my workspace.
- I am aware that some websites and social networks have age restrictions and I should respect this.
- I will not attempt to visit Internet sites that I know to be banned by the school.
- I will only e-mail people I know, or a responsible adult has approved.
- The messages I send, or information I upload, will always be polite and sensible.
- I will not open an attachment, or download a file, unless I know and trust the person who has sent it.
- I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless a trusted adult has given permission. I will never arrange to meet someone I have only ever previously met on the Internet, unless my parent/carer has given me permission and I take a responsible adult with me.
- If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will show a teacher / responsible adult.

I have read and understand these rules and agree to them.

Signed: _____ Date: _____