Oswald Road Primary School

Acceptable Use Policy

Approved by Governing Body: September 2024

To be reviewed in 2 years: September 2026

Headteacher: Deborah Howard

Chair of Governors: Peter Martin

Contents

1. This Policy

This policy applies to any computer or other device connected to the school's network or used on site.

We believe information and communications technology (ICT) includes all forms of computing, the internet, telecommunications, digital media and mobile phones. School personnel have clear responsibilities with regard to the use of all ICT equipment and ICT facilities.

ICT is an integral part of the way our school works, and is a critical resource for pupils, staff, governors, volunteers and visitors. It supports teaching and learning, pastoral and administrative functions of the school. However, the ICT resources and facilities our school uses also pose risks to data protection, online safety and safeguarding.

Any member of the school personnel that uses illegal software or access inappropriate websites when in school, or with school owned devices outside of school, faces dismissal. All school personnel will be made aware of all legislation relating to computer misuse, data protection and copyright.

We expect all school personnel to sign and date the 'Acceptable Use of ICT Agreement' and any other hardware loan agreements relevant to their role. All school personnel have the duty to be fully aware of and implement the internet safety policy and report any misuse of the ICT equipment / ICT facilities of this school.

We believe it is essential that this policy clearly identifies and outlines the roles and responsibilities of all those involved in the procedures and arrangements that is connected with this policy. Where the Headteacher is named, these responsibilities can be delegated to other senior staff.

This policy refers to, and complies with, the following legislation and guidance:

- Data Protection Act 2018
- The UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020
- Computer Misuse Act 1990
- Human Rights Act 1998
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Education Act 2011
- Freedom of Information Act 2000
- Education and Inspections Act 2006
- Keeping Children Safe in Education 2023
- Searching, screening and confiscation: advice for schools 2022
- National Cyber Security Centre (NCSC): Cyber Security for Schools
- Education and Training (Welfare of Children) Act 2021
- UK Council for Internet Safety (et al.) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Meeting digital and technology standards in schools and colleges

2. Aims

This policy aims to:

- Set guidelines and rules on the use of school ICT resources for staff, pupils, visitors, governors, parents and carers.
- Establish clear expectations for the way all members of the school community engage with each other online.
- Support the school's policies on data protection, online safety and safeguarding.
- Prevent disruption that could occur to the school through the misuse, or attempted misuse, of ICT systems.
- Support the school in teaching pupils safe and effective internet and ICT use.

3. Roles & Responsibilities

Role of the Governing Body

The Governing Body has:

- appointed a member of staff to be responsible for ICT and online safety;
- delegated powers and responsibilities to the Headteacher to ensure all school personnel and stakeholders are aware of and comply with this policy;
- responsibility for ensuring funding is in place to support this policy;
- responsibility for ensuring full compliance with all statutory responsibilities;
- responsibility for ensuring that the school complies with all equalities legislation;
- responsibility for the effective implementation, monitoring and evaluation of this policy;
- responsibility for ensuring this policy and all policies are maintained and updated regularly;
- nominated a link governor to visit the school regularly, to liaise with the Headteacher and to report back to the Governing Body.

Role of the Headteacher and School Leadership Team

The Headteacher and the School Leadership Team will:

- review and amend this policy, taking into account new legislation, government guidance and previously reported incidents, to improve procedures;
- ensure the day-to-day implementation and management of this policy by making it widely available;
- maintain a Fixed Asset Register to record and monitor the school's assets, including a log of all ICT equipment used and allocated to school personnel;
- oversee purchase requests for electronic devices, monitoring purchases made under the Finance Policy;
- ensure all school personnel sign the 'Acceptable Use of ICT Agreement' & any other relevant agreements;
- provide guidance, support and training (including at induction) to all staff when the need arises;

- monitor and review the effectiveness of this policy, devising and updating acceptable use guidelines;
- undertake risk assessments when required;
- handle complaints regarding this policy as outlined in the school's Complaints Procedures Policy;
- annually report to the Governing Body on the success and development of this policy.

Role of the ICT Technician

The ICT technician is responsible for:

- carrying out checks on internet activity of all user accounts and to report any inappropriate use to the Headteacher and DSL. The school uses Smoothwall monitoring and filtering
- monitoring the computer logs on the school's network and to report any logged inappropriate use to the Headteacher and/or School Business/ Manager;
- remotely viewing or interacting with any of the computers on the school's network. This may be done randomly to implement this policy and to assist in any difficulties;
- ensuring routine security checks are carried out on all school-owned and personal devices that are used for work purposes to check that appropriate security measures and software have been updated and installed;
- ensuring that thorough, appropriate steps are taken to ensure personal information is not seen during security checks and that staff are made aware of the potential risks;
- accessing files and data to solve problems for a user, with their authorisation;
- adjusting access rights and security privileges in the interest of the protection of the school's data, information, network and computers;
- immediately reporting any breach of personal devices to the School Business/ Manager;
- disabling user accounts of staff who do not follow this policy, at the request of the Headteacher;
- assisting staff with authorised use of the ICT facilities;
- assisting the Headteacher in all matters requiring reconfiguration of security and access rights and in all matters relating to this policy.

Role of School Personnel

School personnel will:

- comply with all aspects of this policy and be aware of all other linked policies;
- read and sign the 'Acceptable Use of ICT Agreement' to confirm they understand their responsibilities and what is expected of them when they use school owned and personal devices in school;
- log off/lock screen when finished using a computer;
- protect their username and passwords, not sharing these with anyone else including the school Wi-Fi credentials;
- request permission before using personal devices in school and submit these for security checks;
- ensure any personal devices used for school purposes are encrypted in a manner approved by the DPO;
- engage in any training provided and successfully complete this;
- report misuse of ICT facilities or devices, by staff or pupils, to the Headteacher.

4. Acceptable Use Agreement

I understand that the school network facility is for the good of my professional development, for the development of this school and must be used only for educational purposes or to enable me to carry out my role fully.

I realise that I have a personal responsibility to abide by the set rules and regulations when using the network and I am aware of the consequences if I breach them.

I am aware that by beaching the rules and regulations it may lead to:

- withdrawal of my user access
- the monitoring of how I use the network
- disciplinary action
- criminal prosecution

I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.

Unacceptable Use of ICT Facilities

The following is considered unacceptable use of the school's ICT facilities by any member of the school community. Any breach of this policy may result in disciplinary or behaviour proceedings.

Unacceptable use of the school's ICT facilities includes:

- Using the school's ICT facilities to breach intellectual property rights or copyright
- Using the school's ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Online gambling, inappropriate advertising, phishing and/or financial scams
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate or harmful
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, its pupils, or other members of the school community
- Connecting any device to the school's ICT network without approval from authorised personnel
- Setting up any software, applications or web services on the school's network without approval by authorised personnel, or creating or using any program, tool or item of software designed to interfere with the functioning of the ICT facilities, accounts or data
- Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities
- Causing intentional damage to the school's ICT facilities

- Removing, deleting or disposing of ICT equipment, systems, programmes or information without permission from authorised personnel
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not permitted by authorised personnel to have access, or without authorisation
- Using inappropriate or offensive language
- Promoting a private business, unless that business is directly related to the school
- Using websites or mechanisms to bypass the school's filtering or monitoring
- Engaging in content or conduct that is radicalized, extremist, racist, antisemitic or discriminatory in any other way
- Using personal devices without activating the correct security settings, i.e. numeric passcode or biometrics settings on home screen notifications for any school related business.

Unacceptable Use of the Internet

In line with the above statements, when using the school's internet I will not:

use the internet in such a way that it will bring the school into disrepute

- use inappropriate or illegal websites
- download inappropriate material or unapproved software
- upload or download large capacity files without permission from the ICT technician
- use programmes or software that may allow people to bypass the filtering or security systems
- use inappropriate language
- use language that may provoke hatred against any ethnic, religious or other minority group

produce, send out, exhibit or publish material that will cause offence to anyone

- give my home address, phone number, social networking details or email addresses to pupils or parents – contact with parents will be done through authorised school contact channels only
- divulge any personal information of any other user or that of pupils

divulge my login credentials or passwords to anyone

- use the login credentials or passwords of any other user

use a computer that is logged on by another user

- use any social networking site, except those used by the school
- transfer the images of pupils without prior permission of the Headteacher and from parents

use email for private use but only for educational purposes

- open email attachments from unknown sources
- compromise the Data Protection Act or the law of copyright in any way

These are not exhaustive lists. The school reserves the right to amend the above at any time. The Headteacher will use professional judgement to determine whether any act or behaviour not on the lists above is considered unacceptable use of the school's ICT facilities and/or internet. Where the use of school ICT facilities and/or internet is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the Headteacher's discretion.

The school's network manager manages access to the school's ICT facilities and materials for school staff. This includes, but is not limited to:

- computers, tablets and other devices, including mobile phones
- monitoring the use of the school's ICT facilities and network
- access permissions for certain programmes or files

Staff will be provided with unique log-in/account information and passwords that they must use when accessing the school's ICT facilities and relinquish upon termination of their employment contract.

Staff who have access to files they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the school's network manager or Headteacher.

Staff may not use the school's ICT facilities to store personal non-work-related information or materials (such as music, videos, or photos).

Staff should be aware that use of the school's ICT facilities for personal use may put personal communications within the scope of the school's ICT monitoring activities. Where breaches of this policy are found, disciplinary action may be taken.

Staff should be aware that personal use of ICT (even when not using school ICT facilities) can impact on their employment.

5. Communication & Working Remotely

Use of School Phones and Email Accounts

The school provides each member of staff with an email address. This email account should be used for work purposes only.

All work-related business should be conducted using the email address the school has provided.

Staff must not share their personal email addresses with parents/carers and pupils, and must not send any work-related materials using their personal email account.

Staff must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.

Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents.

Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.

Staff must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient.

If staff receive an email in error, the sender should be informed and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.

If staff send an email in error which contains the personal information of another person, they must inform the School Business Manager immediately and follow our data breach procedure.

Staff must not open email attachments from unknown sources and report anything suspicious to the School Business/Facilities Manager.

Staff must not give their personal phone numbers to parents/carers or pupils. Staff must use phones provided by the school to conduct all work-related business.

School phones must not be used for personal matters.

Staff who are provided with mobile phones as equipment for their role must abide by the same rules for ICT acceptable use.

All other mobile phones must not be used during teaching hours and need to be kept locked away.

School use 3CX phone system and can use this remotely. Information has been provided to users who need to access the remote system

Remote Working

We allow staff to access the school's ICT facilities and materials remotely.

Staff accessing the school's ICT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on-site. Staff must be particularly vigilant if they use the school's ICT facilities outside the school and take such precautions against importing viruses or compromising system security.

Our ICT facilities contain information which is confidential and/or subject to data protection legislation. Such information must be treated with extreme care and in accordance with our data protection policy.

6. Information & Data Security

The school takes steps to protect the security of its computing resources, data and user accounts. However, the school cannot guarantee security. Staff, pupils, parents and others who use the school's ICT facilities should use safe computing practices at all times.

Passwords

All users of the school's ICT facilities should set strong passwords for their accounts and keep these passwords secure.

Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control.

Members of staff or pupils who disclose account or password information may face disciplinary action.

Parents or volunteers who disclose account or password information may have their access rights revoked.

Access to Facilities and Materials

All users of the school's ICT facilities will have clearly defined access rights to school systems, files and devices.

Users should not access, or attempt to access, systems, files or devices to which they have not been granted access. If access is provided in error, or if something a user should not have access to is shared with them, they should alert the school's Headteacher or School Business Manager immediately.

Users should always log out of systems and lock their equipment when they are not in use to avoid any unauthorised access.

Equipment and systems should always be logged out of and closed down completely at the end of each working day.

Social Media Accounts

The school has a social media account. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access the account. Those who are authorised to manage the account must ensure they abide by the school expectations at all times.

Members of staff should make sure their use of social media and other online accounts, either for work or personal purposes, is appropriate at all times and avoid compromising their professional integrity and/or bringing the school into disrepute.

Encryption

The school ensures that its devices and systems have an appropriate level of encryption.

School staff may only use personal devices (including computers and USB drives) to access school data, work remotely, or take personal data (such as pupil information) out of school if they have been specifically authorised to do so by the Headteacher.

Use of such personal devices will only be authorised if the devices have appropriate levels of security and encryption, as defined by the network manager.

Data Protection

The school is responsible for making sure it has the appropriate level of security protection and procedures in place to safeguard its systems, staff and learners. It therefore takes steps to protect the security of its computing resources, data and user accounts. The effectiveness of these procedures is reviewed periodically to keep up with evolving cyber crime technologies.

Staff, pupils, parents/carers and others who use the school's ICT facilities should use safe computing practices at all times. We aim to meet the cyber security standards recommended by the Department for Education's guidance on digital and technology standards in schools and colleges, including the use of:

- Firewalls
- Security features
- User authentication and multi-factor authentication
- Anti-malware software

All personal data must be processed and stored in line with data protection regulations and the school's data protection policy.

Software Updates, Firewalls, and Anti-Virus Software

All of the school's ICT devices that support software updates, security updates, and anti-virus products will be configured to perform such updates regularly or automatically.

Users must not circumvent or make any attempt to circumvent the administrative, physical and technical safeguards we implement and maintain to protect personal data and the school's ICT facilities.

Any personal devices using the school's network must all be configured in this way.

Monitoring and filtering of the school network and use of ICT facilities

To safeguard and promote the welfare of children and provide them with a safe environment to learn, the school reserves the right to filter and monitor the use of its ICT facilities and network. This includes, but is not limited to, the filtering and monitoring of:

- Internet sites visited
- Bandwidth usage
- Email accounts
- Telephone calls
- User activity/access logs
- Any other electronic communications

Only authorised ICT personnel may filter, inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law. The school uses Smoothwall to aid its monitoring across devices.

The school monitors ICT use in order to:

- Safeguard children and staff
- Obtain information related to school business
- Investigate compliance with school policies, procedures and standards
- Ensure effective school and ICT operation
- Conduct training or quality control exercises
- Prevent or detect crime
- Comply with a subject access request, Freedom of Information Act request, or any other legal obligation

Our governing board is responsible for making sure that:

- The school meets the DfE's filtering and monitoring standards
- Appropriate filtering and monitoring systems are in place
- Staff are aware of those systems and trained in their related roles and responsibilities
    - For the leadership team and relevant staff, this will include how to manage the processes and systems effectively and how to escalate concerns
- It regularly reviews the effectiveness of the school's monitoring and filtering systems

The school's designated safeguarding lead (DSL) will take lead responsibility for understanding the filtering and monitoring systems and processes in place.

Where appropriate, staff may raise concerns about monitored activity with the school's DSL and ICT manager.

Protection From Cyber Attacks

The school will:

- Work with governors and the IT department to make sure cyber security is given the time and resources it needs to make the school secure
- Provide training for staff (and include this training in any induction for new starters) on the basics of cyber security, including how to:
  - Check the sender address in an email
  - Respond to a request for bank details, personal information or login details
  - Verify requests for payments or changes to information
- Make sure staff are aware of its procedures for reporting and responding to cyber security incidents
- Investigate whether our IT software needs updating or replacing to be more secure
- Not engage in ransom requests from ransomware attacks, as this would not guarantee recovery of data
- Put controls in place that are:
  - **Proportionate**: the school will verify this using a third-party audit to objectively test that what it has in place is effective
  - **Multi-layered**: everyone will be clear on what to look out for to keep our systems safe
  - **Up to date:** with a system in place to monitor when the school needs to update its software
  - **Regularly reviewed and tested**: to make sure the systems are as effective and secure as they can be
- Back up critical data frequently and store these backups securely
- Delegate specific responsibility for maintaining the security of our management information system (MIS) to the ICT provider
- Make sure staff:
  - Enable multi-factor authentication where they can
  - Store passwords securely
- Make sure ICT staff conduct regular access reviews to make sure each user in the school has the right level of permissions and admin rights
- Have a firewall in place that is switched on
- Check that its supply chain is secure, for example by asking suppliers about how secure their business practices are and checking if they have the Cyber Essentials certification
- Develop, review and test an incident response plan with the IT department including, for example, how the school will communicate with everyone if communications go down, who will be contacted and when, and who will notify Action Fraud of the incident. After any significant event, the NCSC's 'Exercise in a Box' will be used.

7. Loss, Theft & Damage

The ICT technician will be contacted if a school-owned electronic device has a technical fault.

For the purpose of this policy, **"damage"** is defined as any fault in a school-owned electronic device caused by the following:

- Connections with other devices, e.g. connecting to printers which are not approved by the ICT technician
- Unreasonable use of force
- Abuse
- Neglect
- Alterations
- Improper installation

Any incident that leads to a school-owned electronic device being lost will be treated in the same way as damage.

The school's insurance will cover school-owned electronic devices that are damaged or lost. Staff members will use school-owned electronic devices within the parameters of the school's insurance cover – if a school-owned electronic device is damaged or lost the member of staff at fault will likely be responsible for paying.

The ICT technician and Headteacher will decide whether a device has been damaged due to the actions described above. If it is decided that a member of staff is liable for the damage, they will be required to pay the insurance excess of the total repair or replacement cost. A written request for payment will be submitted to the member of staff who is liable to pay for damages.

If the member of staff believes that the request is unfair, they can make an appeal to the Headteacher, who will make a final decision. In cases where the Headteacher decides that it is fair to seek payment for damages, the member of staff will be required to make the payment within six weeks of receiving the request. However, the Headteacher may accept the payment in instalments.

If the payment has not been made after six weeks, the fee may increase and disciplinary procedures could begin. The member of staff may not be permitted to access school-owned electronic devices until the payment has been made.

In cases where a member of staff repeatedly damages school-owned electronic devices, the Headteacher may decide to permanently exclude the member of staff from accessing devices.

If a school-owned device is lost or stolen, or is suspected of having been lost or stolen, the DPO will be informed as soon as possible to ensure the appropriate steps are taken to delete data from the device that relates to the school, its staff and its pupils, and that the loss is reported to the relevant agencies.

The school will not be responsible for the loss, damage or theft of any personal device, including phones, cameras, tablets, removable media, etc.

8. Pupils

The school will use the behavior policy, if a pupil engages in any of the following **at any time** (even if they are not on school premises):

- Using ICT or the internet to breach intellectual property rights or copyright
- Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination

- Breaching the school's policies or procedures
- Any illegal conduct, or making statements which are deemed to be advocating illegal activity
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
- Consensual or non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams (also known as sexting or youth produced sexual imagery)
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, other pupils, or other members of the school community
- Gaining or attempting to gain access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities
- Causing intentional damage to the school's ICT facilities or materials
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user and/or those they share it with are not supposed to have access, or without authorisation

- Using inappropriate or offensive language
- Use AI in an inappropriate or offensive way

Pupil's Personal Electronic Devices

Mobile phones, tablets and other personal electronic devices have become widely available and accessible to pupils. The school accepts that personal mobile phones and tablets are often given to pupils by their parents to ensure their safety and personal security, but understands that such devices pose inherent risks and may jeopardise the learning environment.

As a school, we must strike a balance between personal safety and a suitable educational setting. We understand that parents may wish for their child to carry a mobile phone for their personal safety, whilst pupils may wish to bring additional devices to school for other reasons.

Pupils are responsible for their own belongings. The school accepts no responsibility for replacing property that is lost, stolen or damaged either on school premises or travelling to and from school, and at school events. Pupils are responsible for replacing school property they lose, damage or steal, including electronic devices.

Pupils and staff should enable a personal PIN or passcode on all the devices they bring to school to protect their personal data, images and videos in the event that the device is lost, stolen or accessed by an unauthorised person.

Only pupils walking to and/or from school without an adult should have personal electronic devices on their possession. Any pupil bringing personal electronic devices into school must make their parents aware of this. All personal electronic devices will be switched off and handed in to class teachers at the start of each day. These will be locked away and only returned to pupils as they are leaving the grounds at the end of the day. No personal electronic devices will be used or accessible during the school day.

All personal electronic devices will be used in line with our Online Safety Policy. Incidents of cyberbullying will be dealt with and reported in line with the Anti-bullying Policy and the Behaviour Policy. As part of the school's ongoing commitment to the prevention of cyberbullying, regular teaching and discussion about online safety will take place as part of PSHE lessons.

Pupils are required to comply with any request to check their electronic device. Failure to do so may result in said device being confiscated. Confiscated personal electronic devices will be locked away securely in the Headteacher's office and will need to be collected by the pupil's parent. A future ban on bringing in any electronic devices may also be made.

9. Parents & Visitors

Parents and visitors do not have access to the school's ICT facilities as a matter of course.

However, an appropriate level of authorisation and/or supervision may be granted by the Headteacher.

The Headteacher will only grant an appropriate level of authorisation if:

- Parents are working with the school in an official capacity (e.g. as a volunteer or as a member of the PTA)
- Visitors need to access the school's Wi-Fi in order to fulfil the purpose of their visit (for instance, to access materials stored on personal devices as part of a presentation or lesson plan)

Parents and visitors to the school are not permitted to use the school's Staff Wi-Fi and where access to the internet is needed, the Visitor Wi-Fi credentials should be shared.

Where parents and visitors are granted access in this way, they must abide by this policy as it applies to staff.

Staff must not give the Staff Wi-Fi password to anyone who is not authorised to have it. Doing so could result in disciplinary action.

10. Equality Impact Assessment

Under the Equality Act 2010 we have a duty not to discriminate against people on the basis of their age, disability, gender, gender identity, pregnancy or maternity, race, religion or belief and sexual orientation.

This policy has been equality impact assessed and we believe that it is in line with the Equality Act 2010 as it is fair, it does not prioritise or disadvantage any pupil/ staff member and it helps to promote equality.

11. Monitoring The Effectiveness Of The Policy

The Headteacher and School Business Manager will monitor the implementation of this policy, including ensuring it is updated to reflect the needs and circumstances of the school.

The practical application of this policy will be reviewed annually or when the need arises by the nominated link governor, Headteacher and/or School Business/Facilities Manager.

The Governing Board is responsible for reviewing and approving this policy. A statement of the policy's effectiveness and the necessary recommendations for improvement will be presented to the Governing Body for further discussion and endorsement.

12. Related Polices & Links

This policy should be read alongside the school's policies and links on:

- Online Safety
- Pupil Mobile Phone Policy
- Safeguarding & Child Protection
- Behavior
- Disciplinary & Dismissal Policy
- Data Protection Procedures

Appendix 1: Acceptable Use Agreement – EYFS/KS1

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS

When I use the school's ICT systems (like computers) and get onto the internet in school I will:

- Ask a teacher or adult if I can do so before using them
- Only use websites that a teacher or adult has told me or allowed me to use
- Tell my teacher immediately if:
    - I click on a website by mistake
    - I receive messages from people I don't know
    - I find anything that may upset or harm me or my friends
- Use school computers for school work only
- I will be kind to others and not upset or be rude to them
- Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly
- Only use the username and password I have been given
- Try my hardest to remember my username and password
- Never share my password with anyone, including my friends.
- Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer
- Save my work on the school network
- Check with my teacher before I print anything
- Log off or shut down a computer when I have finished using it

I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.

Appendix 2: Acceptable Use Agreement – KS2

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS

I will read and follow the rules in the acceptable use agreement policy

When I use the school's ICT systems (like computers) and get onto the internet in school I will:

- Always use the school's ICT systems and the internet responsibly and for educational purposes only
- Only use them when a teacher is present, or with a teacher's permission
- Keep my username and passwords safe and not share these with others
- Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer
- Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others
- Always log off or shut down a computer when I'm finished working on it

I will not:

- Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Log in to the school's network using someone else's details
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision

If I bring a personal mobile phone or other personal electronic device into school:

- I will not use it during lessons, tutor group time, clubs or other activities organised by the school, without a teacher's permission
- I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online

I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.

Appendix 3: Acceptable Use Agreement For Staff, Governors, Volunteers & Visitors

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS,VOLUNTEERS AND VISITORS
When using the school's ICT facilities and accessing the internet in school, or outside school on a work device, I will not: ● Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) ● Use them in any way which could harm the school's reputation ● Access social networking sites or chat rooms ● Use any improper language when communicating online, including in emails or othermessaging services ● Install any unauthorised software, or connect unauthorised hardware or devices to the school's network ● Share my password with others or log in to the school's network using someone else's details ● Share confidential information about the school, its pupils or staff, or other members of the community ● Access, modify or share data I'm not authorised to access, modify or share ● Promote private businesses, unless that business is directly related to the school
I understand that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

Appendix 4 - Personal Electronic Devices Agreement

Pupil personal electronic devices agreement

I understand that bringing a personal electronic device to school is a privilege that may be taken away if I abuse it. I agree to not use my device in school and hand it in each morning. If I use my device in an unacceptable manner, it may be confiscated.

Parent personal electronic devices agreement

I recognise that **Oswald Road Primary School** bears no responsibility for personal electronic devices lost, damaged or stolen on school property or on journeys to and from school.

I agree to the terms of this policy and will discuss the responsibility of owning a personal electronic device with my child.

I understand that devices are not to be used on school grounds and that a teacher may confiscate any devices used in an unacceptable manner.

Appendix 5 – Hardware Loan Agreement For Staff

Oswald Road Primary School, has agreed to provide iPad tablets and Laptops for designated members of the teaching staff. It has also been agreed that one of these tablets/laptops should be assigned to **NAME, ROLE**.

NAME and Oswald Road Primary School hereby agree as follows:

1. The iPad tablet identified below shall be loaned to **NAME** for his / her personal use. The loan shall terminate when **NAME** ceases to be employed at Oswald Road Primary School, unless the school deems the loan to be terminated by breach of conditions in which case it will terminate forthwith. On the termination of the loan, the iPad tablet shall be returned to the school.
2. **NAME** shall be solely responsible for the safe keeping and upkeep of the iPad tablet and shall be liable for making good any loss of or damage to the iPad tablet. **NAME** will make his/ her personal home insurer aware of the nature / value of this equipment and that Oswald Road Primary School is the owner of the iPad and will have an interest in any insurance claim lodged by **NAME** in respect of the iPad tablet. **NAME** is aware of the level of risk s/he undertakes by virtue of this provision.
3. **NAME** agrees to abide by Manchester City Council and Oswald Road Primary School's policies in respect of:

   observance of requirements in respect of the Data Protection Act 1998

   (see https://www.gov.uk/data-protection/the-data-protection-act), in particular the specific requirements under the Act imposed by the school's registration with the Information Commissioner.

   NAME will in addition take all reasonable steps to ensure that any other user of the iPad will also abide by these requirements.
4. **NAME** agrees to pay any telephone or telecommunication charges incurred in connecting the iPad tablet to private or public networks, except in the case of connection to the Local Area Network of any school in connection with professional duties. **NAME** understands that the supply and use of consumables used at home are the teacher's responsibility.
5. In the event of the iPad requiring repair, **NAME** will return the iPad tablet to Oswald Road Primary School for collection and repair by the supplier and will arrange for such collection and repair. **NAME** undertakes not to attempt any such repair him / herself. In this event, **NAME** agrees that software repair may be limited to restoration of the tablet's original software image and therefore that responsibility for regular backup of data and validation of backups rests with **NAME**. Oswald Road Primary School's ICT staff will facilitate such backups and validation, for example by appropriate connections to the school's Local Area Network.
6. **NAME** undertakes not to install any software on the iPad tablet without the written sanction of Oswald Road Primary School. **NAME** further undertakes not to install any Internet Service Provision (other than that provided with the iPad tablet) without the written permission of Oswald Road Primary School, which shall not be granted without consultation with appropriate officers of Education IT Services. **NAME** will ensure that the iPad anti-virus software is regularly updated and will cooperate in maintaining the Oswald Road Primary School anti-virus policy. **NAME** will produce the iPad if requested by Oswald Road Primary School.
7. **NAME** and Oswald Road Primary School agree that the teacher may use the iPad tablet for any purpose s/he wishes, provided solely that it shall not result in personal financial gain for the teacher or any of his/her family or associates, but the expectation shall be that such purpose shall primarily be for the teacher's personal and professional development in connection with her/his duties in the school and always in accordance with all policies and procedures.