

# Acceptable Use Policy (AUP)

## Yew Tree Primary School



<b>Date of Policy:</b>	January 2026
<b>Responsibility:</b>	Reena Kaur - E-Safety Leader
<b>Review Date:</b>	January 2027
<b>Consultation:</b>	This policy was reviewed in consultation with staff, parents and governors taking account of the latest DfE safeguarding and cyber-security arrangements

### ETHOS STATEMENT

It is the aim of the Governing Body of Yew Tree Primary School to develop policies and procedures which support the school's vision of:

***“Learning Without Limits”***

### INTRODUCTION

In order to exploit the many educational and social benefits of new technologies, learners and staff need opportunities to create, collaborate, communicate and explore in the digital world, using multiple devices from multiple locations. School staff are also now actively encouraged to use platforms such as Twitter, Dojo and the website. However, at times, the use of IT for these purposes may encounter risks.

It is now recognised that e-safety risks are posed more by behaviours and values online than the technology itself. Therefore, the approach must be one of empowering pupils and staff to develop safe and responsible behaviours to safeguard themselves and others rather than restricting access to the use of various technologies. We attempt to continually keep up-to-date with the latest e-safety risks posed both in and out of school.

### AIMS

The purpose of this policy is to:

- Establish the ground rules we have in school for using various technologies;
- Offer guidelines which will safeguard and protect pupils and staff from misuse of technology;
- Raise awareness of e-safety among pupils and staff;
- Ensure all staff comply with GDPR legislation.

The school believes that the benefits to pupils and staff from access to the range of technology available far exceed the disadvantages. Ultimately, the responsibility for setting and conveying the standards that we expect in relation to use of technologies is one we share with parents and carers.

The guidance and regulations outlined in this policy will, if adhered to, help to ensure that our infrastructure is a robust and secure one which will offer numerous benefits to all users.

## **USE OF TECHNOLOGY**

All users (pupils and staff) are encouraged to make use of the school's computing facilities for educational purposes. Technology such as mobile phones, tablets, MP3 players, Personal Digital Assistants (PDA), memory cards, encrypted USB storage devices, digital or video cameras should be used responsibly and in accordance with the principles outlined in this policy, even if not connected to the school network. All users must take responsibility for their own use of new technologies, making sure that they use technology safely, responsibly and legally. They must be active participants in e-safety education, taking personal responsibility for their awareness of the opportunities and risks posed by new technologies.

## **NETWORK SECURITY**

All staff and pupil users of the school network are issued with login access to the school network. Protection of login accounts is the responsibility of the individual and passwords should not be shared **in any circumstances**. All users have a duty to protect their passwords and personal network logins and should log off or lock their network account when leaving workstations unattended. Any attempts to access, corrupt or destroy other users' data or compromise the privacy of others in any way, using any technology, is unacceptable.

The security of our network and associated web based programmes, (e.g. SIMs, Office 365) is of paramount importance due to the data that it has stored. Users are reminded that Yew Tree Primary School reserves the right to monitor the network activity and communication within sites procured for school services. This also includes monitoring of any personal and private communications made via the school network. Any misuse of the network and its facilities may result in the user having their account suspended and possible disciplinary action.

The servers have systems in place to back up data and prevent the introduction of a virus to the network. As a result, access to these is limited to the IT Team (SIPS). Permission must be sought from the IT Team for anyone else wishing to access the servers. Pupils **MUST NOT** access the server at any time.

Finally, all users have a duty to respect the technical safeguards which are in place and should not attempt to introduce a virus or malicious code or bypass any network security systems. Any attempt to breach technical safeguards, conceal network identities or gain unauthorised access to the systems and services is unacceptable. It is the duty of all users to report any suspected or known failings in technical safeguards which may become apparent when using the systems and services.

In order to protect the safety and security of our network, users are reminded that they must not download or install any software/hardware or attempt to use any form of hacking systems to gain access to an unauthorised area.

## **ACCESSING THE INTERNET**

The internet is used commonly throughout all aspects of the curriculum both by pupils and by staff. Every effort is made to safeguard users in this environment and pupils are spoken to regularly about e-safety so that they can browse this medium safely and sensibly making decisions about the appropriateness of the material they come across.

Yew Tree Primary School uses a filtered internet service, which will minimise the chances of pupils encountering undesirable material. The filtering service is managed by SIPS (Sandwell) IT Services.

Yew Tree Primary School will only allow pupils to use the internet when there is a responsible adult present to supervise. However, it is unrealistic to suppose that the teacher's attention will always be directed toward the computer/device screen. Pupils are therefore reminded of responsible internet use and the acceptable use agreement (see appendix 1).

Pupils are taught what to do if something appears on the screen that they are unsure about or do not like. The pupil will be asked to turn the monitor screen off and tell an adult straight away.

The use of public chat rooms and /or messaging services is not allowed unless prior permission has been obtained from the head teacher. This may be granted in cases where it is used to support educational activity. In this case school users must not use their personal account and should, instead, create a school based account.

## **USE OF EMAIL/SOCIAL NETWORKING**

All members of staff have access to an individual email account and are required to check them each working day. There is the opportunity for classes to have email accounts if required/needed and staff can arrange this in consultation with the IT Team. Email is recognised as an effective and powerful form of communication and awareness is therefore raised of general email netiquette (see appendix 2). Parents wishing to correspond via email should be directed to the enquiry email address: [enquiries@yewtree.sandwell.sch.uk](mailto:enquiries@yewtree.sandwell.sch.uk) or the Dojo site which is maintained for our school community. If staff communicate with parents/carers via email/Dojo they must maintain the professionalism that would be evident if they were speaking with the parent/carer in person. Any issues should immediately be reported to the Head teacher/Deputy Head teacher.

The use of social networking sites, e.g. Facebook, is strictly forbidden on the school network unless specific permission has been given. The school has a Twitter account so allows and encourages use of this on the school network. However, pupils' knowledge about the correct usage of these platforms is raised through regular e-safety lessons. Staff choosing to access social networking sites should not use this as a form of communication with any pupil. This is imperative in the interests of safeguarding for both staff and pupil.

Use of such networking sites, both within and outside of school, should not bring the individual, Yew Tree Primary or Sandwell LA into disrepute. All users have a responsibility to report any known misuse of technology including the unacceptable behaviour of others.

If a user receives an offensive or upsetting email, then this should be stored and shared with the Head teacher or Deputy Head teacher immediately.

## **USE OF OTHER TECHNOLOGIES**

### **WI-FI ACCESS**

Wi-Fi access is available throughout the school and school owned devices can be securely connected to our network using this facility. Personal devices may be connected to the network with prior permission but must strictly adhere to the same rules.

### **MOBILE PHONES/COMMUNICATION DEVICES**

Staff must NEVER communicate with pupils or parents/carers via the use of personal mobile phones. Any staff found sharing their personal phone numbers with pupils may face disciplinary action.

No communications device, whether school provided or personally owned, may be used for the bullying or harassment of others in any form. This applies to staff and pupil use. All users should be aware that in certain circumstances where unacceptable use is suspected, enhanced monitoring and procedures may come into action, including the power to check and/or confiscate personal technologies such as mobile phones. Staff should not use personal mobile phones to take photographs of pupils, unless specific permission has been granted by the head teacher.

### **CAMERAS**

At Yew Tree we encourage the use of digital imagery by both pupils and staff as it has many uses including use for assessment evidence, display around the school, sharing with parents/press etc. and displaying on the website/Twitter. However, pictures of pupils will only be used in external circumstances (e.g. website or press) with the prior permission of parents or carers (see SIMS/office for current list of permissions for photographs). All lists granting permission will be in accordance to GDPR. Staff must only use school owned devices when taking pictures of children unless specific permission has been granted otherwise.

### **PRINTING/PHOTOCOPYING**

Staff are provided with colour and black and white printing/copying facilities. All users are encouraged to consider the need to print colour documents and to avoid any wastage by carefully selecting the printer they intend to print to and also setting up the print and release system. User printing/copying levels can be logged and monitored.

Staff should not share their user access codes with other members of staff for the photocopier and must remember to log out when they have finished using this facility. Exceptions can be made if a member of staff is asked to collect printing/copy for another member of staff. However, use of the details without the staff member's permission is forbidden.

### **LAPTOPS/iPADS**

A number of staff are provided with a school laptop, iPad or other device for them to use throughout the duration of their employment at Yew Tree Primary School. These may be connected to the school network via individual user accounts and may also be taken off site for staff to complete school work at home.

Staff use of the device is bound by the terms and conditions outlined in the 'IT Loan Agreement' which is signed upon receipt of the device(s). Individual staff are responsible for the device assigned to them and may not exchange this with another member of staff.

Staff adherence to the acceptable use agreement (appendix 1) must also be obtained annually to remind staff of their responsibilities when using technologies for their professional role. Devices assigned to staff may also be used for personal reasons except where this violates the terms and conditions of use or of the AUP.

Software must not be uninstalled or removed from the individual laptop or device in the same way that it must not be installed without the prior permission of the Head Teacher (or relevant subject leader) or IT Team. If staff require apps to be downloaded onto school iPads, they should gain permission from the head teacher (or relevant subject leader) who will authorise and then pass on to the IT Team.

If an IT issue arises, it must be logged with the helpdesk following the details on our website: [www.yewtreeprimary.co.uk/it-support-links](http://www.yewtreeprimary.co.uk/it-support-links). If a staff member feels an issue has not been dealt with, they can email the head teacher or school business manager their concerns.

### **USING AI RESPONSIBLY**

- It is recommended that personal data is not used in generative AI tools as all data entered will be stored.
- Content can be inaccurate and biased with low quality images or out of date so staff need to use their professional judgement when using these and check for appropriateness and accuracy.

### **DOCUMENT STORAGE:**

All users of the network have an individual folder/drive where they can store their personal documents. This drive is only accessible by the individual user and the administrator of the network. Yew Tree also utilises shared drive areas called 'One Drive' which are available via Office 365.

Staff are permitted to use encrypted USB storage devices in order to back up any of their data but must be aware of the guidelines about the storage of pupil data and the need to keep this secure. The use of any unencrypted USB storage devices is strictly prohibited; other methods of accessing school data via an encrypted connection at home have been provided by Yew Tree Primary School (One Drive).

### **MAINTENANCE OF TECHNOLOGY FACILITIES**

Technical support is provided by SIPS IT Team in order to ensure that the computing facilities at this school effectively support teaching and learning. All users have a duty to report faults or issues, in the way described above, as soon as they occur.

All users should use network technologies responsibly. Wasting staff effort or networked resources, or using resources in such a way as to diminish the service for other network users, is unacceptable.

Users should not attempt to repair any equipment themselves and should not attempt to use any equipment which may be dangerous to do so. The subject leader and/or the IT Team can be contacted if you have any questions about the use of any new technologies.

## **DISCIPLINARY PROCEDURES**

Those who misuse technologies or who break the acceptable use agreements may be subject to disciplinary procedures.

## **KEY RESPONSIBILITIES**

### **FOR PUPILS**

- Take notice of and follow any rules & restrictions explained by teachers.
- Take responsibility for keeping themselves and others safe.
- Take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
- Behave sensibly when using any particular technology in order to limit any risks.
- Respect the feelings, rights and values of others.
- Seek help from a trusted adult if things go wrong, and support others who may be experiencing e-safety/cyberbullying issues.
- Discuss e-safety with parents/carers in an open and honest way.

### **FOR STAFF**

- Contribute to the development of e-safety policies.
- Read and agree to the rules outlined in the Acceptable Use Agreement.
- Take responsibility for the security of systems and data.
- Have an awareness of e-safety issues and how they relate to the pupils in their care.
- Model good practice in using new and emerging technologies, emphasising positive learning opportunities rather than focussing on negatives.
- Embed e-safety education in curriculum delivery wherever possible.
- Know how and when to escalate e-safety issues.
- Maintain a professional conduct in their personal use of technology, both within and outside school.
- Take personal responsibility for their professional development in this area.
- Comply with the requirements of the GDPR legislation.

### **FOR THE SENIOR LEADERSHIP TEAM**

- Develop and promote an ethos where e-safety is clearly valued.
- Support the e-safety leader to ensure the development of an e-safety culture.
- Make appropriate resources available to support the development of an e-safe culture.
- Support/handle appropriately incidents of misuse of technologies.
- Take ultimate responsibility for e-safety incidents.
- Monitor compliance with GDPR legislation across the school.

### **FOR THE E-SAFETY LEADER**

- Develop an e-safe culture and act as a point of contact for all e-safety issues (under the direction of the SLT and/or Designated Safeguarding Lead).
- Promote e-safety to all users and support them in their understanding of the issues.
- Ensure that e-safety is embedded into CPD for staff and curriculum coverage for learners.
- Ensure that e-safety is promoted to parents and carers.
- Report e-safety incidents to SLT/DSL as they happen by logging on CPOMS.
- Develop an understanding of the relevant legislation, liaise with the LA or other appropriate bodies and review/update e-safety procedures on a regular basis.

### **FOR THE IT TEAM**

- Support the school in the implementation of e-safety procedures and practices.
- Provide support to the technical infrastructure to support e-safe practices while still maximising learning opportunities.
- Take responsibility for ensuring back-up systems are working and that data is stored securely on the school network.

### **STAFF CONSULTATION**

All staff are governed by the terms of the 'Acceptable Use Agreement'. All staff including teachers, supply staff, learning support assistants and support staff, will be provided with a copy of this policy.

Staff should be aware that network usage can be monitored and traced to the individual user. Discretion and professional conduct is essential.

The monitoring of network usage is a sensitive matter. Staff who operate monitoring procedures should work in consultation with the Senior Leadership Team, particularly where a misuse of the School's Network has been identified.

### **COMPLAINTS**

- Responsibility for handling incidents will be delegated to a senior member of staff.
- Any complaint about staff misuse must be referred to the Head teacher/Deputy Head teacher.
- Pupils and parents/carers will be informed of the complaints procedure.
- Parents/carers and pupils will need to work in partnership with staff to resolve issues.
- There may be occasions when the police must be contacted.
- Early contact could be made to establish the legal position and discuss strategies.
- Sanctions available include:
  - interview/counselling by senior member of staff;
  - informing parents or carers;
  - removal of internet or computer access for a period of time.



## Appendix 1 – STAFF AUP

### Summary of Roles and Responsibilities

*To ensure that staff are fully aware of their responsibilities with respect to Computing use, they are asked to sign this Acceptable Use Agreement.*

- I understand that the network is the property of the school and agree that my use must be compatible with my professional role.
- I understand that the school computing systems may be used for private purposes where this does not breach the terms and conditions of the AUP.
- I understand that the activity on school equipment/infrastructure, or in some cases personal, which falls into the following categories may be deemed as inappropriate. Members of staff or individuals, accessing our IT systems or network, who are found to have breached this policy or attempted to do so will be dealt with under the school's disciplinary procedure. Furthermore, this could lead to criminal prosecution as well as dismissal. Accessing, browsing or searching for, storing, downloading or forwarding any materials, be they text, image, audio or data which could be considered:
  - Obscene
  - Offensive
  - Sexual
  - Politically offensive
  - Of a nature which may bring Yew Tree Primary School or the individual into disrepute.
  - An inappropriate contribution to a newsgroup, chat room or other similar medium.
  - As running a private business, e.g. selling or advertising in a way which conflicts with your work at Yew Tree Primary School.
  - An infringement of copyright (including images, text, music or video in any format)
  - An attempt to circumnavigate the security and protection in place on the networks or computers.
- I will respect computing systems security and understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.
- I understand and agree that school will monitor the network and internet use to ensure policy compliance.
- I will not install any software or hardware without permission.
- I will not disclose any password or login name to anyone, other than, where appropriate, the staff responsible for maintaining the system. I will lock my account or log off whenever I am leaving a computer unattended.
- I will take all reasonable precautions to secure data or equipment taken off the school premises and report any compromises immediately to the Head teacher/Deputy Head teacher.
- I will not let any family members, or non-school personnel use school computing equipment which has been loaned to me.

- I will report any incidents of concern to the school Designated Safeguarding Lead (named in the Child Protection & Safeguarding Policy) as appropriate and log it on CPOMS.
- I will ensure that my electronic communications with pupils and parents/carers are compatible with my professional role and cannot be misinterpreted. I will behave in line with communication protocols provided.
- I will promote e-safety with the pupils that I work with and will help them to develop a responsible attitude to computing use.
- Disposal of software/hardware used by the school shall only be carried out through the agreed arrangements for the school and I recognise that this will need to be signed off by the School Business Manager/Governors. Any equipment disposed of in any other way may be deemed as theft.
- I will respect copyright and intellectual property rights.
- I shall take reasonable precautions to safeguard myself and the pupils in my care and shall therefore not communicate with pupils via social networking sites or by sharing mobile phone numbers.
- I shall report any faults/damage of computing equipment to the IT Helpdesk and I understand that jobs will then be prioritised. I shall not attempt to fix any faults myself.
- I shall carefully consider whether it's necessary to print a document so that my printing does not become excessive or lead to unnecessary waste of resources.
- I shall ensure I have a full understanding of, and comply with, GDPR legislation.

The school may exercise its right to monitor the use of the school's computer systems, including access to websites, the interception of e-mail and the deletion of inappropriate materials, where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I understand that inappropriate use of the school computing facilities may lead to disciplinary procedures being implemented.

<b>SIGNED:</b>	
<b>PRINT NAME:</b>	
<b>DATE:</b>	

## Appendix 1 – PUPIL AUP



### Summary of Roles and Responsibilities

I agree that I will:

- Always keep my passwords a secret
- Only visit websites which are appropriate and useful to my learning
- Tell my teacher or an adult I trust if anything from the internet makes me feel scared or upset, or if I feel it is inappropriate
- Make sure any messages I send are polite and respectful
- Not send or reply to any 'nasty' messages using email, Facebook, Snapchat or other similar sites (whether in or out of school)
- Not bring my mobile phone to school if I have one (unless previously agreed with the head teacher) and only give my telephone number to people I know and trust
- Only use the login account I have been provided with at school and make sure I log out when I have finished
- Always keep my personal details private and not share them with other people on the internet
- Not put photographs of myself or others on the internet without checking with an adult first
- Not arrange to meet anyone I 'met' on the internet without discussing it with an adult I trust
- Not install my own software onto school computers
- Respect and look after school computing equipment and report any faults to my class teacher

I understand that everything I do on the computers at school is monitored and that inappropriate behaviour or misuse of ICT equipment will not be tolerated!

I also understand that things I do online outside of school can be traced so I need to act responsibly.

I know who I need to speak to if I am aware of ICT equipment being used in the wrong way by anyone else.

<b>NAME:</b>	<b>DATE:</b>
--------------	--------------

### PARENTAL ACKNOWLEDGEMENT

I have read through the Acceptable Use Agreement for pupils and know the rules that my child is asked to adhere to. I will support the school in enforcing these rules so that my child accesses technology in an e-safe manner.

<b>SIGNED:</b>	<b>DATE:</b>
----------------	--------------

## Appendix 2



### ***EMAIL NETIQUETTE***

Netiquette refers to the generally accepted rules of behaviour for using the internet. Netiquette rules mainly apply to email and are intended to make the internet a civil place to communicate and share ideas.

- Be clear and concise
- Be pleasant and polite
- Include the topic for your message in the subject area
- Never create or forward a 'chain letter' email
- Verify the recipients before sending an email
- To avoid long distribution lists or to hide private addresses use the BCC (blind carbon copy) section of an email
- Avoid using all capital letters in a message as this could be perceived as threatening
- Don't say something in an email that you wouldn't say or be prepared to discuss in person
- Remember to check your email regularly and discard any unwanted messages from your inbox
- Reply promptly to emails (even if you just acknowledge the receipt of an email)
- Consider what you write in emails as all records of communication are bound by the General Data Protection Regulations and are available in the public domain once published (even if deleted).



## Yew Tree Primary School Agreement for Loan of Laptop IT Equipment

**Yew Tree Primary School** has agreed to provide funded devices for designated members of the staff in order to support them in their role/to support the educational development for pupils at our school.

\_\_\_\_\_ and **Yew Tree Primary School** hereby agree as follows:

The devices identified below shall be loaned to **THE NAMED PERSON** for his/her personal use. The loan shall terminate when **THE NAMED PERSON** ceases to be employed at **Yew Tree 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 device shall be returned to the School.

The device is covered by insurance provided by the school except for loss, theft or damage occasioned by the negligence of **THE NAMED PERSON** such as leaving the device prominent in an unattended car, in which case any such loss or damage shall be made good at the expense of **THE NAMED PERSON**. **THE NAMED PERSON** is aware of the level of risk s/he undertakes by virtue of this insurance cover.

**THE NAMED PERSON** agrees to abide by **Yew Tree Primary School's** policies in respect of

- Observance of requirements of GDPR legislation which, in practice, means that teachers consider information available on their laptops or devices which makes an individual identifiable. If they do hold this information (e.g. assessment data exported from SIMS), they need to exercise great care in keeping their work under a secure user password, which is not known to other users of the laptop such as family members.
- Acceptable Use Policy (Internet/Home Network/Public Networks)
- Health and safety of **THE NAMED PERSON** or any other individual
- Child protection & Safeguarding and E-safety

**THE NAMED PERSON** will in addition take all reasonable steps to ensure that any other user of the device will also abide by these requirements.

**THE NAMED PERSON** agrees to pay any telephone or telecommunication charges incurred in connecting the device to private or public networks, except in the case of connection to the Local Area Network of any school in connection with professional duties. **THE NAMED PERSON** understands that the supply and use of consumables used at home are the teacher's responsibility.

In the event of the device requiring repair, **THE NAMED PERSON** will return the device to **Yew Tree Primary School** for collection and repair by the IT Team who will arrange for such collection and repair. **THE NAMED PERSON** undertakes not to attempt any such repair him/herself. In this event, **THE NAMED PERSON** agrees that software repair may be limited to restoration of the computer's original software image and therefore that responsibility for regular backup of data and validation of backups rests with **THE NAMED PERSON** (unless it is information stored on the network). **Yew Tree Primary School's** IT staff will facilitate such backups and validation, for example by appropriate connections to the school's Local Area Network.

**THE NAMED PERSON** undertakes not to install any software on the laptop without the written sanction of **Yew Tree Primary School**. **THE NAMED PERSON** will ensure that the device anti-virus software is regularly updated and will cooperate in maintaining the **Yew Tree Primary School** anti-virus policy. **THE NAMED PERSON** will produce the device if requested by **Yew Tree Primary School** for anti-virus checking and updating if required to do so.

**THE NAMED PERSON** and **Yew Tree Primary School** agree that the staff member may use the device 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 professional development or duties in connection with their role in the school. For example, planning, preparation and assessment and that both parties shall collaborate in recognising what activities might produce outcomes beneficial to both the teacher and the school. To this end, **Yew Tree Primary School** will endeavour to provide any training mutually agreed to be necessary.

---

**Schedule of Loan:**

Laptop Computer – Make .....

Model.....

Serial number.....

School Inventory Reference: .....

iPad Device – Make .....

Model.....

Serial number.....

School Inventory Reference: .....

Mobile Phone – Make .....

Model.....

Serial number.....

School Inventory Reference: .....

Staff name: \_\_\_\_\_

Role: \_\_\_\_\_

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

Authorised by **J. Barry** on behalf of **Yew Tree Primary School**

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

---

Returned and Checked by: (print name)

Reason for return: .....

Signature.....