WISHFORD EDUCATION

IT ACCEPTABLE USE POLICY

This policy applies to all Wishford Education settings including schools, nurseries and camps.

Responsible Person: Head of Compliance	
Last Review	**Significant changes (most recent updates in red)**
July 2024	**Updated to include name change to Wishford Education**
September 2024	**All references now made role rather than person specific.**

1. Policy Scope

Wishford Education is committed to the acceptable and responsible use of technology by all members of their schools, nurseries and camps (settings) communities.

The aims of this policy are:

- To safeguard and promote the welfare of all members of The Wishford community in relation to the use of technology.
- To protect the group's systems & data.
- To control and protect the settings' channels of communication.

This policy should be read in conjunction with the Privacy Notice & **Data Protection Policy, Online Safety Policy and Staff Handbook**. Other related policies include:

- Safeguarding policy
- Anti-Bullying policy
- Behaviour and discipline policy
- Curriculum policies, such as: Personal Social Health and Economic Education (PSHE) and Relationships and Sex Education (RSE)

This policy was written with regard to external guidance including:

- Keeping Children Safe in Education;
- The Early Years and Foundation Stage;
- Working Together to Safeguard Children;
- Behaviour in Schools: Advice for headteachers and school staff;
- Searching, screening and confiscation at school;
- Teaching online safety in schools;

This policy applies to pupils and all parents, visitors and staff; including the governing body, leadership team, teachers, support staff, external contractors, volunteers and other individuals who work for, or provide services on behalf of the setting, e.g. guest speakers.

This policy applies to the use of any 'device' which can access the internet, access or store setting information, communicate with other accounts/devices or take photographs/video/audio recordings **(**collectively referred to as **"devices"** in this policy). If users are unsure whether their device is captured by this policy they should check with the IT department before using their device on-site.

It is implicit within this policy that staff and pupils should endeavour to use setting devices to carry out setting related activities whenever possible. This policy applies to both **setting-owned** and **privately-owned** devices. It also relates to the use of technology **on and off site, at all times of the day.**

Staff compliance with this policy is an important part of the setting's compliance with the Data Protection Act 2018. Staff must apply this policy consistently with the group's Privacy Notice & Data Protection Policy.

All members of each setting's community should be updated at least **annually** on the guidance outlined in this policy. It forms part of the induction process for all new staff, parents and pupils. Pupils will be educated regarding the safe and appropriate use of technology and will be made aware of behaviour expectations and consequences for policy breaches on, at least, an annual basis.

This policy is updated at least once every five years or following any relevant local or national updates or changes in our technical infrastructure. Internal monitoring and risk assessment may also lead to policy updates. Settings will be notified whenever the policy is updated. Staff and pupils have to sign the relevant Acceptable Use Agreement below upon joining the setting or following any significant updates to this policy.

2. Staff Agreement IT Acceptable Use: Staff Agreement

This agreement relates to all employees, contractors, volunteers and other individuals who work for, or provide services on behalf of Wishford Education. These users must also read the group's Online Safety policy and Privacy Notice & Data Protection policy. By engaging in your role, you agree to recognise/adhere to the following guidelines (as well as all other related policies) when using technology in any way, at all times:

a. Conduct. Staff must:

i. Ensure that their online communications, and any shared content, are respectful of others and composed in a way they would wish to stand by.
ii. Not access, create or share content that is illegal, deceptive, or likely to offend others (e.g. content that is obscene, violent, discriminatory, extreme or raises safeguarding issues).
iii. Respect the privacy of others and not share photos, videos, contact details, or other information about others without going through official channels and obtaining permission.
iv. Not access/share material that infringes copyright or claim the work of others as their own.
v. Not use the internet to distribute malicious software, to damage, interfere with, or gain unauthorised access to the computer systems of others, or carry out related illegal activities.

b. Usage (all devices). Staff must:

i. Avoid the use of personal email/social media accounts for setting business/to contact pupils/parents.
ii. Not represent their personal views as being that of the Setting.
iii. Use auto lock/passwords/PIN on devices to avoid unauthorised access, calls or actions.
iv. Only use their accounts and maintain a private and regularly updated password (at least 8 characters and include 3 of: lower case, upper case, number & non-alphabetical (e.g.! $, %). Ideally, staff follow National Cyber Security Centre advice and use 3 random words.
v. Enable MFA (Multi Factor Authentication) for their work email account.
vi. Safeguard against phishing/malware/ransomware emails by immediately deleting unknown/untrusted emails/links/attachments and informing the IT helpdesk.
vii. Respect Wishford IT equipment and report any damage/fault to the IT helpdesk immediately.
viii. Not access banking & payment services via the setting's WIFI without authorisation.
ix. Not download apps/software onto setting devices without authorisation.
x. Never attempt to bypass any security controls embedded in IT systems.
xi. Ensure that appropriate, up-to-date security software is installed on their devices.
xii. Report data protection issues immediately to the Head & dataprotection@wishford.co.uk.
xiii. Report the receipt of any inappropriate/illegal content immediately to their Head.
xiv. Ensure guest teachers/speakers adherence to this policy (whenever possible, 'presentations' should be sent to the member of staff in advance to check content and to allow use of a Wishford device).
xv. Notify their Head immediately if they consider that any content shared on their personal social media sites conflicts with their role.
xvi. Be aware that the group cannot guarantee the confidentiality of content created, shared and exchanged via group systems.
xvii. Contact helpdesk@schooldomain.com if they are unsure about any content or usage.

c. Usage (personal devices):

i. Staff wishing to use their personal device during on-site activity agree to only access the internet via the setting's Wi-Fi at all times.
ii. Staff must ensure that personal devices are:
- Fully up to date with the latest software updates.
- Supported by their manufacturer.
- Not being hacked or have been hacked which would allow to access organisational data.
- Not known to contain any viruses and are running up to date anti-virus with at least daily definition updates (where applicable)

iii. Staff can use personal devices in the presence of groups children for:
- Work related activity but only when a setting device is less effective or unavailable.
- Personal activity but only in emergencies and following a discussion with the Head.

iv. Staff must always keep their devices hidden and silent in the following situations:
- When working 1to1 with a pupil.
- When working in any location where intimate care takes place: e.g. toilets, changing rooms and the EYFS.

v. Staff should otherwise consider the necessity of personal device usage at all other times.
vi. Staff agree to share their current usage whenever asked to do so by a member of SLT.
vii. Staff must not make personal use of images/film taken of pupils or setting activity.
viii. Staff must remove any setting data from personal accounts, cloud storage, drives or devices at the earliest possible convenience.

d. Wishford Accounts

Alongside the general staff agreement above, members of staff responsible for their setting's website and social media channels must also agree to the following guidance:

i. Personal information should not be posted on any setting's website and only official email addresses should be used to identify members of staff.
ii. Settings will not create individual social media profiles for any member of their community.
iii. Staff with access to their setting's social media accounts must complete regular training on the acceptable use of social media.
iv. Official social media activity use will be conducted in line with existing policies, including but not limited to Anti-Bullying and Safeguarding.
v. All communication on official social media platforms by staff on behalf of the setting will be clear, transparent and open to scrutiny. Public communications on behalf of the setting will, where appropriate and possible, be read and agreed by at least one other colleague.
vi. Settings will ensure that any official social media use does not exclude members of their community who are unable or unwilling to use social media channels.
vii. Official social media sites must be suitably protected and linked to the setting's website.
viii. Official social media channels must be set up as distinct and dedicated accounts for official educational or engagement purposes only.
ix. Staff will use setting email addresses to register for and manage official social media channels.
x. The Head must have access to account information and login details for any social media channels.
xi. Staff are advised to safeguard themselves and their privacy. This may include, but is not limited to:
    i. Setting appropriate privacy levels on each account;
    ii. Being aware of the implications of using location sharing services;
    iii. Opting out of public listings;
    iv. Logging out of accounts after use;
    v. Using strong passwords;
xii. Members of staff managing and/or participating in online social media activity, as part of their capacity as an employee of the setting, will:
    i. Read and understand this policy and their setting's Staff Code of Conduct.
    ii. Be aware they are an ambassador for their setting.
    iii. Be professional, responsible, credible, fair and honest, and consider how the information being published could be perceived or shared.
    iv. Always act within the legal frameworks they would adhere to within the workplace, including libel, defamation, confidentiality, copyright, data protection and equalities laws.
    v. Ensure that appropriate consent has been given before sharing images. Written permission from parents or carers will be obtained before photographs of students/pupils are published on the setting's website/social media/local press.
    vi. Take care when taking digital/video images that students/pupils are appropriately dressed and are not participating in activities that might bring the individuals or the setting into disrepute.
    vii. Never use a pupil's full name alongside their image.
    viii. Not disclose information, make commitments or engage in activities on behalf of the setting, unless they are authorised to do so.
    ix. Inform the DSL (or a Deputy) and/or the Head of any concerns, such as criticism, inappropriate content or contact from pupils.

Print Name: ……. **Signed:** ……... **Date:** ……

3. Pupil agreement

IT Acceptable Use: Pupil Agreement

N.B. Settings have the scope to adapt this agreement to be more age appropriate or align with programmes of study. However, the fundamental principles of the agreement should be covered within any adaptation.

At all times, I will:

- Keep my personal device silent and hidden at my setting unless given permission to do otherwise by a teacher.
- Accept the setting's right to monitor my online activity and devices.
- Avoid any unnecessary printing.
- Not try to bypass the group's internet filtering.
- Not use social media **during non-boarding hours**.

When using group's systems/devices, I will:

- Take good care of setting devices and never knowingly risk damaging/evading school hardware/software.
- Immediately report any damage or problems with setting devices.
- Use group systems and devices for work only and not attempt to modify and hardware or software.
- Not download anything, open attachments or use USB/memory hardware when using setting devices.

When using the internet for setting work, I will:

- Never copy the work of others and claim that it is mine
- Check that information I find on the internet is from a reliable website.
- Only use the school's Wi-Fi and never log into a VPN or mobile network on-site.

To keep myself and others safe online, I will:

- Be respectful and kind when using the internet.
- Ensure my personal device has up-to-date virus protection.
- Only download material approved by my parents or teacher.
- Not share any images or information from setting without **written** permission from a teacher.
- Only use websites/accounts that are appropriate for my age.
- Never look at or do anything inappropriate or illegal on the internet.
- Only share my personal information (name, address, family, setting) with known family and friends.
- Never share the personal information of others.
- Never share any images/recordings of others on the internet without their permission.
- Keep safe/secure passwords, logout of accounts after use, use multi-factor authentication if necessary.
- Not share my log-in with anyone or try to use/change other people's accounts.
- Be suspicious of unexpected contacts and messages.
- Not arrange to meet any stranger who has contacted me over the internet.
- Report any unpleasant material or messages sent to me, including any cyber-bullying incidents.
- Not attempt to discover or contact the personal email addresses or social media accounts of other pupils or **Wishford Education** staff and to report any unauthorised access immediately.

☐ **I agree to this Acceptable Use agreement**

☐ **I accept there will be appropriate consequences if I do not comply with this agreement.**

Setting	
Full Name & Year Group	
Date	

4. Visitors Agreement

Visitors is a broad term which covers any person who is not a pupil or employee of the setting, for example, parents/carers, external contractors or guest speakers.

By entering our site, all visitors agree to the guidelines below. If you are unable to adhere to these guidelines please inform a member of staff immediately:

N.B. Settings should add the following guidance to any visitor welcome information.

a. Family members are allowed to photograph/record setting performances (i.e. sports fixtures, assemblies or performing arts productions) which include their child.
b. Family members should not share images/recordings taken at the setting on any publicly accessible platform.
c. In no other circumstances should visitors take images/recordings of children unless given permission to do so by a member of staff.
d. Visitors should report any damage to a personal device to the setting office.
e. Visitors accept that the setting and Wishford take no responsibility for the physical and digital security of their personal devices whilst on-site.
f. Visitors should report any data breach or conduct concerns immediately to the setting office.
g. Family members/visitors should not attempt to discover or contact the personal email addresses or social media accounts of staff.

6. Monitoring

a. Wishford Education reserves the right to monitor and access the web history and/or email use of any pupil or member of staff.
b. Any personal devices used by pupils, whether or not such devices are permitted, may be confiscated and examined in line with the 2011 Education Act.
c. The Group may require staff to conduct searches of their personal accounts or devices if they were used for Wishford business in contravention of this policy, and if there is any reason to suspect illegal activity or any risk to the wellbeing of any person. Staff devices may be confiscated for an investigation into a policy breach (see below).
d. The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students/pupils when they are off the setting site and empowers members of staff to impose disciplinary penalties for inappropriate off-site behaviour.

7. Policy Breach

The Head should be aware of, authorise and risk assess (when appropriate to do so) all breaches to this policy. Unauthorised breaches to this policy are subject to the following guidance:

a. All members of staff are advised that their online conduct on personal social media can have an impact on their role and reputation within the setting. Civil, legal or disciplinary action may be taken if staff are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities. All members of staff are encouraged to carefully consider the information, including text and images, they share and post online.
b. An unauthorised breach of this policy by staff or pupils will be dealt with as a disciplinary (and pastoral) matter in line with the Safeguarding, Staff Code of Conduct, Disciplinary, Anti-Bullying and Behaviour policies.
c. The DSL (or a Deputy) will respond to concerns involving safeguarding or safeguarding risks in line with our Safeguarding policy.
d. Concerns regarding pupils' acceptable use will be shared with parents/carers as appropriate.
e. The Head is responsible for imposing any reasonable sanctions for an unauthorised breach. When the Head deems it necessary to impose a sanction, they will seek advice from Wishford leadership and any relevant external agencies as appropriate.
f. Sanctions range from temporarily restricting access to group IT systems to contacting the police for suspected illegal activity. When deemed necessary, the Head reserves the right to formally suspend/exclude a pupil and oversee a formal disciplinary procedure for a member of staff.
g. All adults have a responsibility to report concerns. Parents/visitors and staff should contact the Head if they have any concern about a breach of this policy (and Wishford directly if the concern is regarding the Head's conduct). Staff should be familiar with the group's Whistleblowing policy.
h. When investigating an alleged breach, the Head will adhere to the following procedure:
    i. More than one senior member of staff will be involved in the process. This is vital to protect individuals if accusations are subsequently reported.
    ii. The procedure will be conducted using a designated computer that will not be used for any other purpose and if necessary can be taken off site by the police should the need arise. The same computer will be used for the duration of the procedure.
    iii. The investigating staff will have appropriate internet access to conduct the procedure, but will also ensure that the sites and content visited are closely monitored and logged.
    iv. The URL of any site containing the alleged misuse will be logged including a description of the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the investigation file (except in the case of images of child sexual abuse – see below).
    v. Once this has been completed and fully investigated the Head will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
        - Internal response or discipline procedures.
        - Involvement by Local Authority or national organisation (as relevant).
        - Police involvement and/or action.

If content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police are listed below. In all cases, isolate the computer in question as best you can. Any change to its state may hinder a later police investigation:

- incidents of 'grooming' behaviour.
- the sending of obscene materials to a child.
- adult material which potentially breaches the Obscene Publications Act.
- criminally racist material.
- promotion of terrorism or extremism.
- offences under the Computer Misuse Act (see User Actions chart above).
- other criminal conduct, activity or materials.

vi. It is important that all of the above steps are taken as they will provide an evidence trail for the setting and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed file should be retained by the group for evidence and reference purposes.

Appendix 1: Unacceptable online activity

The following table is not an exhaustive list of all possible online activity. However, it does give users a good guide regarding the levels of unacceptable usage. Unacceptable usage can range from accessing websites which are not age/role appropriate (e.g. a pupil accessing social media whilst on-site) to illegal activity.

N.B. Illegal activity must be reported to the police. Under the Cyber-Prevent agenda the National Crime Agency has a remit to prevent young people becoming involved in cyber-crime and harness their activity in positive ways – further information here

User Actions	Acceptable for nominated users and only at certain times	Unacceptable	Unacceptable and illegal
Activities that might be classed as cyber-crime under the Computer Misuse Act.			X
Gaining unauthorised access to group networks, data and files, through the use of computers/devices		X	
Creating or propagating computer viruses or other harmful files			X
Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)			X
Disable/Impair/Disrupt network functionality through the use of computers/devices		X	
Using penetration testing equipment (without relevant permission)		X	
Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978 N.B. Settings should refer to guidance about dealing with self-generated images/sexting – UKSIC Responding to and managing sexting incidents and UKCIS – Sexting in schools and colleges			X
Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.			X
Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008			X
Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986			X
Pornography		X	

Promotion of any kind of discrimination			X
threatening behaviour, including promotion of physical or mental harm			X
Promotion of extremism or terrorism			X
Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the setting or brings the setting into disrepute		X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the setting		X	
Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords)		X	
Unfair usage (downloading/uploading large files that hinders others' usage)		X	
Using group systems to run a private business		X	
Infringing copyright			X
On-line gaming (educational)	X		
On-line gaming (non-educational)		X	
On-line gambling		X	
On-line shopping/commerce	X		
File sharing	X		
Use of social media	X		
Use of messaging apps	X		
Use of video broadcasting e.g. Youtube	X		

Appendix 2: Policy Breach Investigation Log

Setting:	
Date:	
Details of first reviewing person (inc role)	
Details of second reviewing person (inc role)	
Reason for investigation (inc pupils/staff involved)	
Name and location of computer used for review	
Log of websites visited/activity undertaken during review	
Outcomes of review process Action taken/proposed	