Witton Gilbert Primary School

# Acceptable Use Policy

| | |
|---|---|
| **Date Policy Written** | March 2022 |
| **Date agreed and ratified by Governing Body** | |
| **Date of next review** | |
| **Named Governor with lead responsibility** | Mrs J Swinbank |
| **Designated Safeguarding Leads** | Mrs P Nelson (HT)<br>Mrs K Curry (DHT) |
| **Computing Lead Teacher** | |
| **ICT Technician** | Mr R Cooper |

# Contents

# 1. Introduction and aims

Information and communications technology (ICT) is an integral part of the way our school works, and is a critical resource for pupils, staff (including senior leadership teams), 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.

This policy aims to:

- Set guidelines and rules on the use of school ICT resources for staff, pupils, parents and governors
- Establish clear expectations for the way all members of the school community engage with each other online
- Support the school's policy on data protection, online safety and safeguarding
- Prevent disruption 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

This policy covers all users of our school's ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors.

Breaches of this policy may be dealt with in differing ways, taking into consideration who has breached the guidance and the severity of the incident.  The associated policies that may be used in these cases include the school behaviour policy, disciplinary policy and staff code of conduct.

# 2. Relevant legislation and guidance

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

- Data Protection Act 2018
- The General Data Protection Regulation
- 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
- The Education and Inspections Act 2006
- Keeping Children Safe in Education 2021
- Searching, screening and confiscation: advice for schools
- National Cyber Security Centre (NCSC)
- Education and Training (Welfare of Children Act) 2021

# 3. Definitions

- **"ICT facilities":** includes all facilities, systems and services including but not limited to network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, and any device system or service which may become available in the future which is provided as part of the ICT service
- **"Users":** anyone authorised by the school to use the ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors
- **"Personal use":** any use or activity not directly related to the users' employment, study or purpose
- **"Authorised personnel":** employees authorised by the school to perform systems administration and/or monitoring of the ICT facilities
- **"Materials":** files and data created using the ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites and blogs

See appendix 6 for a glossary of cyber security terminology.

# 4. Unacceptable use

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 (see section 4.2 below).

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 (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, 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 ICT facilities
- Removing, deleting or disposing of ICT equipment, systems, programs or information without permission by authorised personnel
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed 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 mechanisms
- Engaging in content or conduct that is radicalised, extremist, racist, anti-Semitic or discriminatory in any other way

This is not an exhaustive list. The school reserves the right to amend this list at any time. The headteacher and Senior Leadership Team will use professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the school's ICT facilities.  This may include discussion with relevant Local Authority services; such as the Digital Safety Support and Compliance Officer.

## 4.1 Exceptions from unacceptable use

Where the use of school ICT facilities (on the school premises and/or remotely) 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. To do so, the person needing such access should request this in writing prior to the date use is required, and before any unacceptable use arises.  Without prior agreement all unacceptable use is not acceptable and exceptions cannot be granted retrospectively.

## 4.2 Sanctions

Pupils and staff who engage in any of the unacceptable activity listed above may face disciplinary action in line with the school's published behaviour policy, disciplinary policy and staff code of conduct. For pupils, repeated incidents of unacceptable use may lead to the revoking of permission to use school's systems and may impact on how we can deliver the full curriculum to meet the individual child's needs.

# 5. Staff (including governors, volunteers, and contractors)

## 5.1 Access to school ICT facilities and materials

The school's ICT Technician works with the School Business Manager to manage access to the school's ICT facilities and materials for school staff. That includes, but is not limited to:

- Computers, tablets, mobile phones and other devices
- 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.

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 ICT Technician via email (as he works in our setting part time). They will be able to update permissions and make note of incidents that occur, offering support and enabling access as appropriate. All staff and pupils should have access to their relevant working areas within the school ICT systems and it is rare that updates are needed; most cases are when staff wish for new or updated technology and programming to be added to the systems.

### 5.1.1 Use of phones and email

The school provides each member of staff with an email address. This email account should be used for work purposes only. Staff should enable multi-factor authentication on their email accounts and 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 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. Advice upon encryption can be sourced from the ICT Technician.

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 that contains the personal information of another person, they must inform the School Business Manager immediately and follow our data breach procedure.

Staff must not give their personal phone numbers to parents or pupils. Staff must use phones provided by the school to conduct all work-related business, unless otherwise pre-arranged with the headteacher (e.g. when staff are providing remote learning from home, when staff conduct telephone meetings from home during PPA time, when multiple members of staff are on an educational visit and need to communicate from different areas of site or in case of emergency – school only has one mobile phone for this purpose). When staff need to make a call to a parent they should always enter the digits 141 before dialling the parental contact number to ensure their personal phone number remains private.

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 as set out in section 4.

## 5.2 Personal use

Staff are permitted to occasionally use school ICT facilities for personal use subject to certain conditions set out below. Personal use of ICT facilities must not be overused or abused. The headteacher may withdraw permission for it at any time or restrict access at their discretion.

Personal use is permitted provided that such use:

- Does not take place during contact time (teaching and learning sessions, assemblies, playtime duties etc.)
- Does not constitute 'unacceptable use', as defined in section 4
- Takes place when no pupils are present

- Does not interfere with their job, or prevent other staff or pupils from using the facilities for work or educational purposes

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 (see section 5.5). Where breaches of this policy are found, disciplinary action may be taken.

Staff are also permitted to use their personal devices (such as mobile phones or tablets) in line with the school's Online Safety policy – mobile phone/personal device section.

Staff should be aware that personal use of ICT (even when not using school ICT facilities) can impact on their employment by, for instance, putting personal details in the public domain, where pupils and parents could see them.

Staff should take care to follow the school's guidelines on social media (see appendix 1) and use of email (see section 5.1.1) to protect themselves online and avoid compromising their professional integrity.

### 5.2.1 Personal social media accounts

Members of staff should ensure their use of social media, either for work or personal purposes, is appropriate at all times.

The school has guidelines for staff on appropriate security settings for Facebook accounts (see appendix 1).

## 5.3 School social media accounts

The school has an official Twitter account @WGPStweets, managed by Katherine Curry, Deputy Headteacher. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access the account.

The school has guidelines for what can and cannot be posted on its social media accounts. Those who are authorised to manage the account must ensure they abide by these guidelines at all times.

## 5.4 Monitoring of school network and use of ICT facilities

The school reserves the right to monitor the use of its ICT facilities and network. This includes, but is not limited to, monitoring of:

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

Only authorised ICT staff may inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law.

The school monitors ICT use in order to:

- Obtain information related to school business
- Investigate compliance with school policies, procedures and standards; in particular safeguarding
- 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

# 6. Pupils

## 6.1 Access to ICT facilities

- Laptop devices and iPads are available to pupils only under the supervision of staff
- This includes specialist ICT equipment, such as that used for music, science or design and technology, which also must only be used under the supervision of staff
- Pupils will be provided with an account linked to the school's virtual learning environment, which they can access within the school building only
- Parents and pupils will be provided with an individual Class Dojo login, which they can use to access school newsletters and information shared by staff and to look at the class pages. Each teacher is responsible for ensuring pupils know that their Class Dojo accounts are for schoolwork purposes only and communication should be in line with the pupil acceptable use policy. Repeated inappropriate use of Class Dojo could lead to the suspension of an account and other means of communication being established for that person.

## 6.2 Search and deletion

Under the Education Act 2011, and in line with the Department for Education's guidance on searching, screening and confiscation, the school has the right to search pupils' phones, computers or other devices for inappropriate images or any other data or items banned under school rules or legislation e.g. pornography.

The school can, and will, delete files and data found on searched devices if we believe the data or file has been, or could be, used to disrupt teaching or break the school's rules.

Staff members may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse contains an online element.

## 6.3 Unacceptable use of ICT and the internet outside of school

The school will sanction pupils, in line with the behaviour policy and online safety policy, if a pupil engages in any of the following **at any time** (in rare cases, 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 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 and 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 ICT facilities or materials
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation
- Using inappropriate or offensive language

# 7. Parents

## 7.1 Access to ICT facilities and materials

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

However, parents working for, or with the school in an official capacity (for instance, as a volunteer or as a member of the Friend of the School ) may be granted an appropriate level of access, or be permitted to use the school's facilities at the headteacher's discretion. Staff should request this permission in writing prior to requiring the ICT use and should be aware that they are responsible for ensuring that the parent follows the acceptable use policy while working within school and is only accessing the required programming.

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

## 7.2 Communicating with or about the school online

We believe it is important to model for pupils, and help them learn, how to communicate respectfully with, and about, others online.

Parents play a vital role in helping model this behaviour for their children, especially when communicating with the school through our website and social media channels.

We ask parents to sign the agreements in appendices 2,3 and/or 4, as appropriate.

# 8. Data security

The school is responsible for making sure it has the appropriate level of security protection and procedures in place. It therefore 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.

## 8.1 Passwords

All users of the school's ICT facilities should set strong passwords for their accounts and keep these passwords secure. Once in KS2, children will set their own school passwords as part of the school online safety curriculum.

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.

Passwords are generated by the school ICT technician, who has access to all passwords for security reasons e.g. in case pupils lose or forget their passwords.

## 8.2 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.

## 8.3 Data protection/GDPR

All personal data must be processed and stored in line with data protection regulations and the school's data protection policy.  The data protection policy can be found on the school website or a paper copy can be requested from the school office.

## 8.4 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.

These access rights are managed by the school ICT Technician.

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 ICT technician 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.

### 8.5 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 ICT technician.

## 9. Protection from cyber attacks

Please see the glossary (appendix 6) to help you understand cyber security terminology.

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 annual training for staff (and include this training in any induction for new starters, if they join outside of the school's annual training window) 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 (such as 360 degree safe via SWGfL) annually, to objectively test that what it has in place is up to scratch
    - **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 up to scratch and secure as they can be
- Back up critical data on the server and NAS boxes on weekdays, which overwrites the week before. Another NAS box undertakes a monthly backup on the first weekend of every month. These are currently stored on the school site and the ICT technician and School Business Manager are looking into offsite, online storage, the cost implications and assessing which data would be stored.
- Delegate specific responsibility for maintaining the security of our management information system (MIS) to our ICT technician; selected elements of the data are shared via offsite programming e.g. CPOMS, Times Table Rockstars and other such safe sites (GDPR compliancy ensured by the School Business Manager), with onsite storage on the physical servers which are stored in a secured part of the building which is not accessible to anyone other than relevant staff.
- Make sure staff:
    - Enable multi-factor authentication where they can, on things like school email accounts
    - Store passwords securely using a password manager
- 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; we use Smoothwall filtration and Panda Adaptive Defense 360
- Implement, review and test the Disaster Recovery Plan, as written by the School Business Manager with the IT department, for example, including how the school will communicate with everyone if communications go down, who

will be contacted when, and who will notify the relevant authorities of the incident. This will be reviewed and tested annually.

- Work with our Local Authority to see what it can offer the school regarding cyber security, such as advice on which service providers to use or assistance with procurement

## 10. Internet access

The school wireless internet connection is secure and uses Smoothwall Monitoring and Filtering to ensure pupil and staff safety. It is set to the highest setting, although some applications and programming is ‘allowed’ to beat the system e.g. the school Twitter account supersedes the block on Social Media applications and is necessary for staff to access, so has been allowed for staff iPads only, as has YouTube access for teaching purposes on staff logins.

The Computing Lead and School Office Manager record and track any incursions to ensure online safety. If staff have repeated incidents of avoidable unacceptable use then they should undergo additional training to remind them of safe practice.

### 10.1 Pupils

Pupils have restricted Wi-Fi access and this is limited to school shared devices only. The children cannot request any enabling of other devices or a change in their safety settings. Their filtration settings are at the highest standard possible and children use Swiggle and Google to enable safe searching online.

If pupils were to have repeated incidents of unacceptable use which were tracked via the filtration settings or misuse identified by a member of staff, they could face sanctions to restrict their access.

### 10.2 Parents and visitors

Parents and visitors to the school will not be permitted to use the school’s Wi-Fi unless specific authorisation is granted by the headteacher.

The headteacher will only grant authorisation if:

- Parents are working with the school in an official capacity (e.g. as a volunteer or as a member of the Friends of the School)
- Visitors need to access the school’s WIFI 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)

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

## 11. Monitoring and review

The headteacher, Computing Lead, ICT Technician and School Business Manager and School Office Manager work as a team to monitor the implementation of this policy, including ensuring it is updated to reflect the needs and circumstances of the school.

This policy will be reviewed every 2 years.

The governing board is responsible for approving this policy and the linked Governors are Mrs M. Harrison (safeguarding) and Mrs J.Swinbank (computing).

## 12. Related policies

This policy should be read alongside the school’s policies on:

- Online safety
- Safeguarding and child protection
- Behaviour
- Staff discipline
- Data protection
- Remote learning

# a. Appendix 1: Social Media cheat sheet for staff

**Don’t accept friend requests from pupils on social media**

## 10 rules for school staff on Facebook (or similar sites)

1. Change your display name – use your first and middle name, use a maiden name, or put your surname backwards instead
2. Change your profile picture to something unidentifiable, or if not, ensure that the image is professional
3. Check your privacy settings regularly
4. Be careful about tagging other staff members in images or posts
5. Don’t share anything publicly that you wouldn’t be just as happy showing your pupils
6. Don’t use social media sites during school hours
7. Don’t make comments about your job, your colleagues, our school or your pupils online – once it’s out there, it’s out there
8. Don’t associate yourself with the school on your profile (e.g. by setting it as your workplace, or by ‘checking in’ at a school event)
9. Don’t link your work email address to your social media accounts. Anyone who has this address (or your personal email address/mobile number) is able to find you using this information
10. Consider uninstalling the Facebook app from your phone. The app recognises Wi-Fi connections and makes friend suggestions based on who else uses the same Wi-Fi connection (such as parents or pupils)

---

## Check your privacy settings

- Change the visibility of your posts and photos to **‘Friends only’**, rather than ‘Friends of friends’. Otherwise, pupils and their families may still be able to read your posts, see things you’ve shared and look at your pictures if they’re friends with anybody on your contacts list
- Don’t forget to check your **old posts and photos** – go to bit.ly/2MdQXMN to find out how to limit the visibility of previous posts
- The public may still be able to see posts you’ve **‘liked’**, even if your profile settings are private, because this depends on the privacy settings of the original poster
- **Google your name** to see what information about you is visible to the public
- Prevent search engines from indexing your profile so that people can’t **search for you by name** – go to bit.ly/2zMdVht to find out how to do this
- Remember that **some information is always public**; your display name, profile picture, cover photo, user ID (in the URL for your profile), country, age range and gender

## What to do if…

### A pupil adds you on social media

- In the first instance, ignore and delete the request. Block the pupil from viewing your profile
- Check your privacy settings again, and consider changing your display name or profile picture
- If the pupil asks you about the friend request in person, tell them that you’re not allowed to accept friend requests from pupils and that if they persist, you’ll have to notify senior leadership and/or their parents. If the pupil persists, take a screenshot of their request and any accompanying messages
- Notify the senior leadership team or the headteacher about what’s happening

### A parent adds you on social media

- It is at your discretion whether to respond. Bear in mind that:
    - Responding to one parent’s friend request or message might set an unwelcome precedent for both you and other teachers at the school
    - Pupils may then have indirect access through their parent’s account to anything you post, share, comment on or are tagged in
- If you wish to decline the offer or ignore the message, consider drafting a stock response to let the parent know that you’re doing so

### You’re being harassed on social media, or somebody is spreading something offensive about you

- **Do not** retaliate or respond in any way
- Save evidence of any abuse by taking screenshots and recording the time and date it occurred
- Report the material to Facebook or the relevant social network and ask them to remove it
- If the perpetrator is a current pupil or staff member, our mediation and disciplinary procedures are usually sufficient to deal with online incidents
- If the perpetrator is a parent or other external adult, a senior member of staff should invite them to a meeting to address any reasonable concerns or complaints and/or request they remove the offending comments or material
- If the comments are racist, sexist, of a sexual nature or constitute a hate crime, you or a senior leader should consider contacting the police

## b. Appendix 2: Acceptable use of the internet: agreement for parents and carers

**Witton Gilbert Primary School**

**Acceptable use of the internet: agreement for parents and carers**

**Name of parent/carer:**

**Name of child:**

Online channels are an important way for parents/carers to communicate with, or about, our school.

The school uses the following channels:

- Our school website
- Class Dojo
- Our official Twitter page
- Email/text for parents (for school announcements and information)

Parents/carers may also set up independent channels to help them stay on top of what's happening in their child's class. For example, class/year Facebook groups, email groups, or chats (through apps such as WhatsApp).

When communicating with the school via official communication channels, or using private/independent channels to talk about the school, I will:

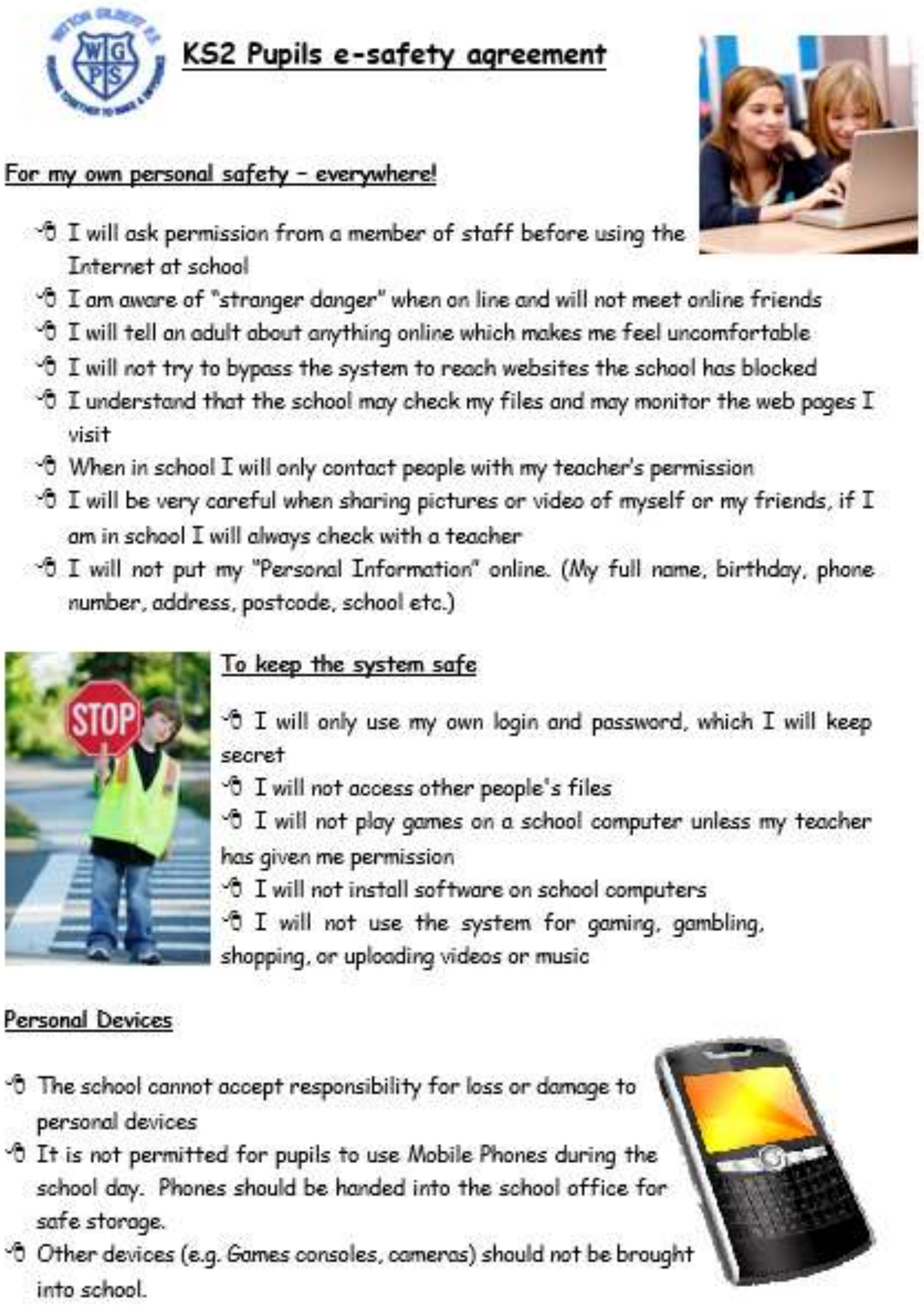
- Be respectful towards members of staff, and the school, at all times
- Be respectful of other parents/carers and children
- Direct any complaints or concerns through the school's official channels, so they can be dealt with in line with the school's complaints procedure

I will not:

- Use private groups, the school's Facebook page, or personal social media to complain about or criticise members of staff. This is not constructive and the school can't improve or address issues if they aren't raised in an appropriate way
- Use private groups, the school's Facebook page, or personal social media to complain about, or try to resolve, a behaviour issue involving other pupils. I will contact the school and speak to the appropriate member of staff if I'm aware of a specific behaviour issue or incident
- Upload or share photos or videos on social media of any child other than my own, unless I have the permission of other children's parents/carers

| | |
|---|---|
| **Signed:** | **Signed:** |

## c. Appendix 3: Acceptable use agreement for older pupils



### KS2 Pupils e-safety agreement

**For my own personal safety – everywhere!**

- I will ask permission from a member of staff before using the Internet at school
- I am aware of "stranger danger" when on line and will not meet online friends
- I will tell an adult about anything online which makes me feel uncomfortable
- I will not try to bypass the system to reach websites the school has blocked
- I understand that the school may check my files and may monitor the web pages I visit
- When in school I will only contact people with my teacher's permission
- I will be very careful when sharing pictures or video of myself or my friends, if I am in school I will always check with a teacher
- I will not put my "Personal Information" online. (My full name, birthday, phone number, address, postcode, school etc.)

**To keep the system safe**

- I will only use my own login and password, which I will keep secret
- I will not access other people's files
- I will not play games on a school computer unless my teacher has given me permission
- I will not install software on school computers
- I will not use the system for gaming, gambling, shopping, or uploading videos or music

**Personal Devices**

- The school cannot accept responsibility for loss or damage to personal devices
- It is not permitted for pupils to use Mobile Phones during the school day. Phones should be handed into the school office for safe storage.
- Other devices (e.g. Games consoles, cameras) should not be brought into school.

**Responsibility to others**

- The messages I send will be polite and responsible
- I will not upload images or video of other people without their permission
- Where work is copyrighted (Including music, videos and images) I will not download it or share with others.
- I understand that the school may take action against me if I am involved in incidents of inappropriate behaviour wherever their location. If the activities are illegal this may be reported to the police.

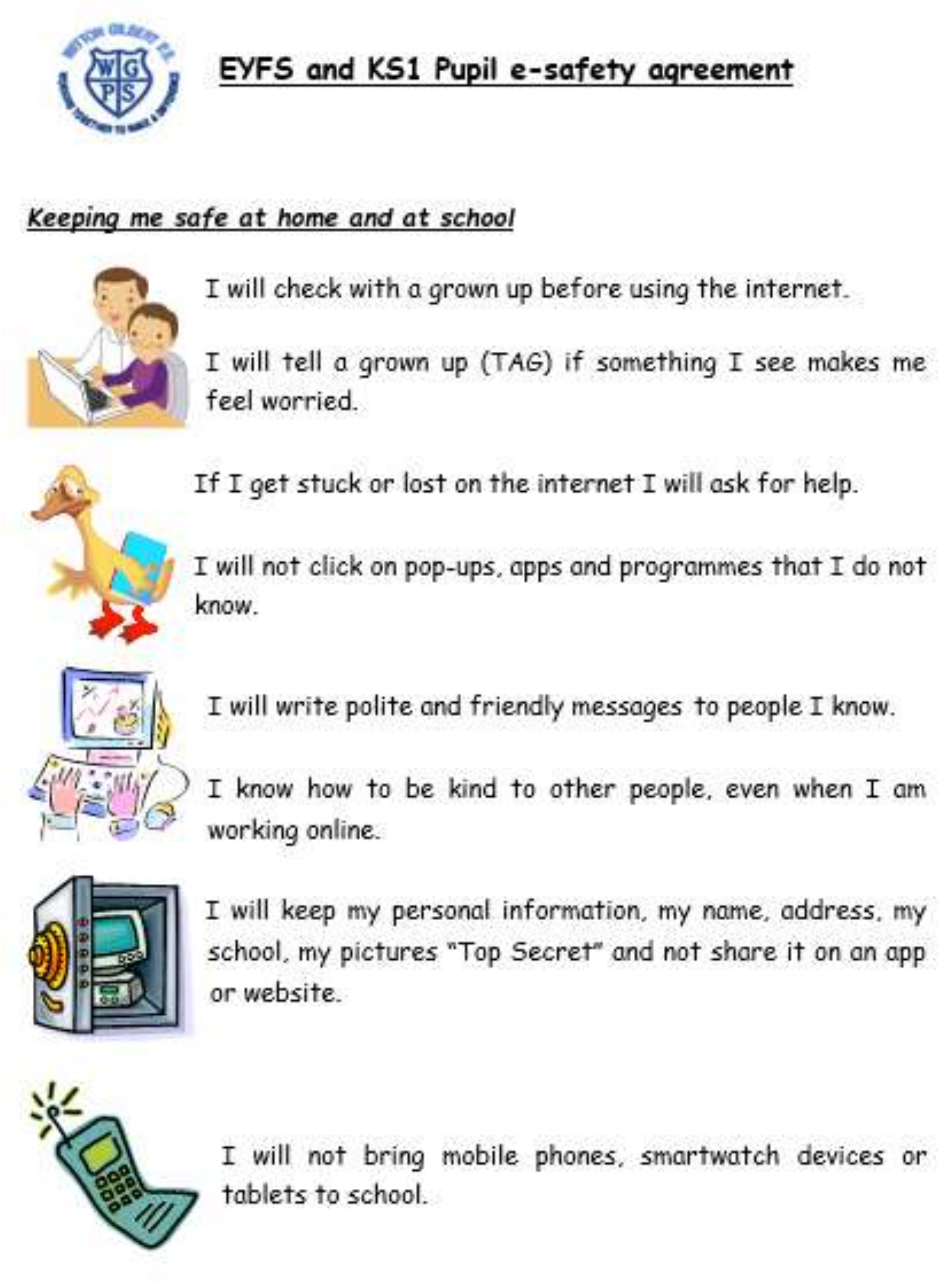
We understand that your child is too young to give informed consent on his/her own; however, we feel it is good practice to involve them as much as possible in the decision making process, and believe a shared commitment is the most successful way to achieve this.

## Pupils e-safety contract

Please complete, sign and return to the school office

| | |
|---|---|
| *Pupil:* | *Form:* |
| **Pupil's Agreement**<br>I have read and I understand the pupils e-safety agreement, and will abide by the rules which are designed to keep both myself and the school safe | |
| *Signed:* | *Date:* |
| Parent's Consent<br>I have read and understood the WGPS e-safety agreement and give permission for my son / daughter to access the Internet while at Witton Gilbert Primary School, and will encourage them to abide by these rules. Children will receive advice on e-safety at school, advice for parents is available at www.thinkuknow.org.uk/parents or by contacting the school. I understand that the school will take reasonable precautions to ensure pupils cannot access inappropriate materials.<br>The school will help children to learn about staying safe online, but recognises that the primary responsibility for online safety at home lies with parents / carers. The school will seek to work with families to help them to encourage children to adopt safe use of the digital technologies at home.<br>I will follow the school's guidance on taking and sharing images and video at school events. | |
| *Signed:* | *Date:* |
| *Please print name:* | |

## d. Appendix 4: Acceptable use agreement for younger pupils



### EYFS and KS1 Pupil e-safety agreement

***Keeping me safe at home and at school***

I will check with a grown up before using the internet.

I will tell a grown up (TAG) if something I see makes me feel worried.

If I get stuck or lost on the internet I will ask for help.

I will not click on pop-ups, apps and programmes that I do not know.

I will write polite and friendly messages to people I know.

I know how to be kind to other people, even when I am working online.

I will keep my personal information, my name, address, my school, my pictures "Top Secret" and not share it on an app or website.

I will not bring mobile phones, smartwatch devices or tablets to school.

We understand that your child is too young to give informed consent on his/her own; however, we feel it is good practice to involve them as much as possible in the decision making process, and believe a shared commitment is the most successful way to achieve this.

## Pupils e-safety contract

Please complete, sign and return to the school office

| | |
|---|---|
| *Pupil:* | *Class:* |

Pupil's *Agreement*

I have listened to and understood the pupils' e-safety agreement, and will follow the rules which are there to keep me and the school safe.

| | |
|---|---|
| *Signed:* | *Date:* |

Parent's Consent

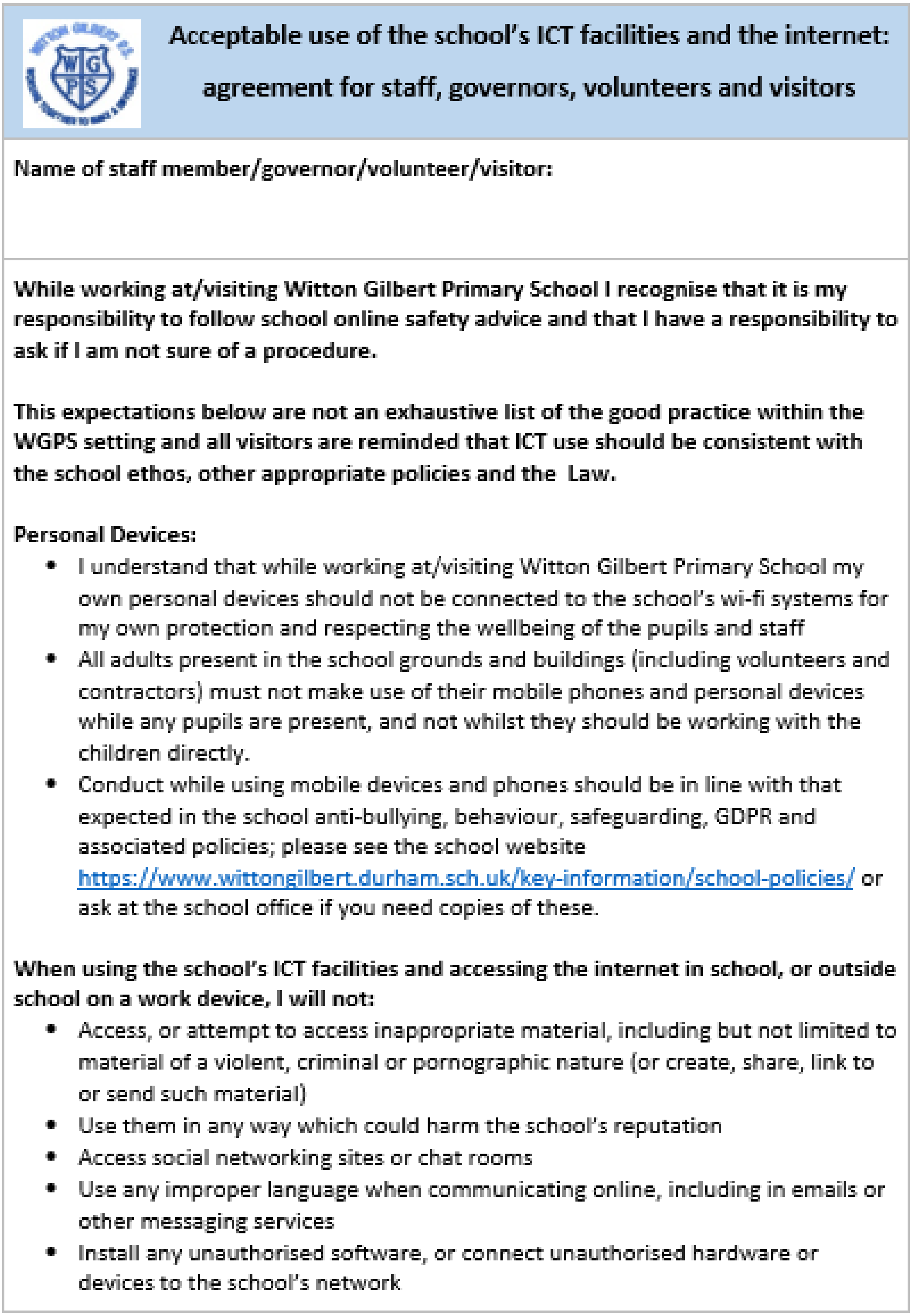
I have read and understood the e-safety agreement and give permission for my son/daughter to access the Internet at school, and will encourage them to abide by these rules. Children will receive advice on e-safety at school, advice for parents is available at www.thinkuknow.org.uk/parents or by contacting the school. I understand that the school will take reasonable precautions to ensure pupils cannot access inappropriate materials and that school will check my child's files and monitor their web access to keep them safe.

The school will help children to learn about staying safe online, but recognises that the primary responsibility for online safety at home lies with parents / carers. The school will seek to work with families to help them to encourage children to adopt safe use of the digital technologies at home.

I will follow the school's guidance on taking and sharing images and video at school events.

| | |
|---|---|
| *Signed:* | *Date:* |
| *Please print name:* | |

## e. Appendix 5: Acceptable use agreement for staff, governors, volunteers and visitors



### Acceptable use of the school's ICT facilities and the internet: agreement for staff, governors, volunteers and visitors

Name of staff member/governor/volunteer/visitor:

**While working at/visiting Witton Gilbert Primary School I recognise that it is my responsibility to follow school online safety advice and that I have a responsibility to ask if I am not sure of a procedure.**

**This expectations below are not an exhaustive list of the good practice within the WGPS setting and all visitors are reminded that ICT use should be consistent with the school ethos, other appropriate policies and the  Law.**

**Personal Devices:**

- I understand that while working at/visiting Witton Gilbert Primary School my own personal devices should not be connected to the school's wi-fi systems for my own protection and respecting the wellbeing of the pupils and staff
- All adults present in the school grounds and buildings (including volunteers and contractors) must not make use of their mobile phones and personal devices while any pupils are present, and not whilst they should be working with the children directly.
- Conduct while using mobile devices and phones should be in line with that expected in the school anti-bullying, behaviour, safeguarding, GDPR and associated policies; please see the school website https://www.wittongilbert.durham.sch.uk/key-information/school-policies/ or ask at the school office if you need copies of these.

**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 other messaging 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.

| | |
|---|---|
| **Signed (staff member/governor/volunteer/visitor):** | **Date:** |

## f. Appendix 6: Glossary of cyber security terminology

These key terms will help you to understand the common forms of cyber-attack and the measures the school will put in place. They're from the National Cyber Security Centre (NCSC) glossary.

| TERM | DEFINITION |
|---|---|
| **Antivirus** | Software designed to detect, stop and remove malicious software and viruses. |
| **Cloud** | Where you can store and access your resources (including data and software) via the internet, instead of locally on physical devices. |
| **Cyber attack** | An attempt to access, damage or disrupt your computer systems, networks or devices maliciously. |
| **Cyber incident** | Where the security of your system or service has been breached. |
| **Cyber security** | The protection of your devices, services and networks (and the information they contain) from theft or damage. |
| **Download attack** | Where malicious software or a virus is downloaded unintentionally onto a device without the user's knowledge or consent. |
| **Firewall** | Hardware or software that uses a defined rule set to constrain network traffic – this is to prevent unauthorised access to or from a network. |
| **Hacker** | Someone with some computer skills who uses them to break into computers, systems and networks. |
| **Malware** | Malicious software. This includes viruses, trojans or any code or content that can adversely impact individuals or organisations. |
| **Patching** | Updating firmware or software to improve security and/or enhance functionality. |
| **Pentest** | Short for penetration test. This is an authorised test of a computer network or system to look for security weaknesses. |
| **Phishing** | Untargeted, mass emails sent to many people asking for sensitive information (like bank details) or encouraging them to visit a fake website. |
| **Ransomware** | Malicious software that stops you from using your data or systems until you make a payment. |
| **Social engineering** | Manipulating people into giving information or carrying out specific actions that an attacker can use. |
| **Spear-phishing** | A more targeted form of phishing where an email is designed to look like it's from a person the recipient knows and/or trusts. |

| TERM | DEFINITION |
|---|---|
| **Trojan** | A type of malware/virus designed to look like legitimate software that can be used to hack a victim's computer. |
| **Two-factor/multi-factor authentication** | Using 2 or more different components to verify a user's identity. |
| **Virus** | Programs designed to self-replicate and infect legitimate software programs or systems. |
| **Virtual Private Network (VPN)** | An encrypted network which allows remote users to connect securely. |
| **Whaling** | Highly targeted phishing attacks (where emails are made to look legitimate) aimed at senior executives. |