

# Kingsthorpe Grove Primary School



## Acceptable use Policy

Person(s) Responsible for Document: Alison Dolan

Date Document Discussed and Agreed with: **5<sup>th</sup> July 2021**

Governor/Relevant Committee: **Standards and Achievement**

Date Document Ratified at Full Governing Body: **15<sup>th</sup> July 2021**

Signed: 

Committee Chair

Signed: 

Chair of Governors

Signed: 

Head Teacher

**Date Document to be reviewed: July 2022**

## Staff and Volunteer Acceptable Use Policy

### School Policy

This Acceptable Use Policy reflects the school online safety policy. The school will ensure that staff and volunteers will have good access to IT to enable efficient and effective working, to enhance learning opportunities for pupils and will, in return, expect staff and volunteers to agree to be responsible users.

At Kingsthorpe Grove we aim to ensure that all of our policies take into account the rights of all children.

Please be aware that sometimes the use of social media can negatively affect children's progress and can negatively affect both children and adults mental health.

### Scope of Policy

This Acceptable User Policy (AUP) policy applies to staff, volunteers, governors and guests who have access to and are users of school IT systems and to school related use of IT systems outside of school.

1. I have read and understood Kingsthorpe Grove's full Online Safety policy and agree to uphold the approaches outlined there, both for my behaviour as an adult and enforcing the rules for pupils/students. I will report any breaches or suspicions (by adults or children) in line with the policy without delay.
2. I understand it is my duty to support a whole-school safeguarding approach and will report any behaviour which I believe may be inappropriate or concerning in any way to the Designated Safeguarding Lead (if by a child) or Headteacher (if by an adult).
3. **During remote learning:**
  - **I will not behave any differently** towards students compared to when I am in school. I will never attempt to arrange any meeting, including tutoring session, without the full prior knowledge and approval of the school, and will never do so directly with a pupil. The same applies to any private/direct communication with a pupil.
  - **I will not attempt to use a personal system or personal login for remote teaching** or set up any system on behalf of the school without SLT approval.
  - **I will not take secret recordings or screenshots** of myself or pupils during live lessons.
  - **I will conduct any video lessons in a professional environment** as if I am in school. This means I will be correctly dressed and in an appropriate room. The camera view will not include any personal information or inappropriate objects and where possible to blur or change the background, I will do.
  - **I will complete a Myconcern for live lessons** if anything inappropriate happens or anything which could be construed in this way. This is for my protection as well as that of students
4. I understand that in past and potential future remote learning and lockdowns, there is a greater risk for grooming and exploitation as children spend more time at home and on devices; I must play a role in supporting educational and safeguarding messages to help with this.
5. I understand the responsibilities listed for my role in the school's Online Safety policy. This includes promoting online safety as part of a whole school approach in line with the **RSHE curriculum**, as well as safeguarding considerations when supporting pupils remotely.
6. I understand that school systems and users are protected by security, monitoring and filtering services, and that my use of school devices, systems and logins on my own devices and at home (regardless of time, location or connection), including encrypted content, can be monitored/captured/viewed by the relevant authorised staff members.

7. I understand that I am a role model and will promote positive online safety and model safe, responsible and positive behaviours in my own use of technology, including social media, e.g. by:
  - not sharing other's images or details without permission
  - refraining from posting negative, threatening or violent comments about others, regardless of whether they are members of the school community or not.
8. I will not contact or attempt to contact any pupil or to access their contact details (including their usernames/handles on different platforms) in any way other than school-approved and school-monitored ways. I will report any breach of this by others or attempts by pupils to do the same to the headteacher.
9. Details on social media behaviour, the general capture of digital images/video and on my use of personal devices is stated in the full Online Safety policy. If I am not sure if I am allowed to do something in or related to school, I will not do it.
10. I understand the importance of upholding my online reputation, my professional reputation and that of the school), and I will do nothing to impair either.
11. I agree to adhere to all provisions of the school Data Protection Policy at all times, whether or not I am on site or using a school device, platform or network, and will ensure I do not access, attempt to access, store or share any data which I do not have express permission for. I will protect my passwords/logins and other access, never share credentials and immediately change passwords every 6 months.
12. I will not store school-related data on personal devices, storage or cloud platforms (except the school's onedrive). USB keys, if allowed, will be encrypted, and I will only use safe and appropriately licensed software, respecting licensing, intellectual property and copyright rules at all times.
13. I will never use school devices and networks/internet/platforms/other technologies to access material that is illegal or in any way inappropriate for an education setting. I will not attempt to bypass security or monitoring and will look after devices loaned to me.
14. I will not support or promote extremist organisations, messages or individuals, nor give them a voice or opportunity to visit the school. I will not browse, download or send material that is considered offensive or of an extremist nature by the school.
15. I understand and support the commitments made by pupils/students, parents and fellow staff, governors and volunteers in their Acceptable Use Policies and will report any infringements in line with school procedures.
16. I will follow the guidance in the safeguarding and online-safety policies for reporting incident: I understand the principle of 'safeguarding as a jigsaw' where my concern might complete the picture. I have read the sections on handling incidents and concerns about a child in general, sexting, upskirting, bullying, sexual violence and harassment, misuse of technology and social media.
17. I understand that breach of this AUP and/or of the school's full Online Safety Policy here may lead to appropriate staff disciplinary action or termination of my relationship with the school and where appropriate, referral to the relevant authorities.

I have read, understood and agreed to this policy. I understand that it is my responsibility to ensure I remain up to date and read and understand the school's most recent online safety / safeguarding policies.

**Signature:**

---

**Name:**

---

**Role:**

---

**Date:**

---

## KS1 Pupil Acceptable Computer and Internet Use Policy

*I understand and agree to follow the KGPS online safety code:*

Kingsthorpe Grove Primary School's Online Safety code: 

**K** ind - Be kind online

**G** enuine - Is it real or fake?  
Is that person who they say they are?

**P** eople - Only meet with and share with people you know

**S** ecure - Keep personal information safe.  
Don't share passwords



**I will talk to a trusted adult if I am worried**

Signed:

## KS2 Pupil Acceptable Computer and Internet Use Policy

*I understand and agree to follow the KGPS online safety code:*

Kingsthorpe Grove Primary School's Online Safety code: 

**K**ind - Show kindness online, promote positivity and be respectful

**G**enuine - Be able to tell the difference between what is real and what is fake. Is it reliable?

**P**eople - Only meet with and share information with people you know

**S**ecure - Keep personal information safe.  
Stay secure with strong passwords

**I will speak to a trusted adult if I am worried about something**

Signed:

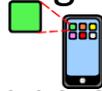
Unit pupils Acceptable use policy



What I Must do to Keep Safe Online and With Devices



Online means anything connected to the internet.



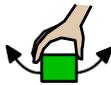
Most devices and apps are connected to the internet.



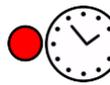
Devices are technology like: computers, laptops,



games consoles, tablets and smart phones.

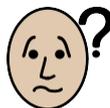
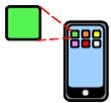


I will only use the devices I am allowed to use.

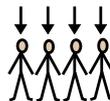


I will ask a trusted adult before I use new websites, games

or apps.



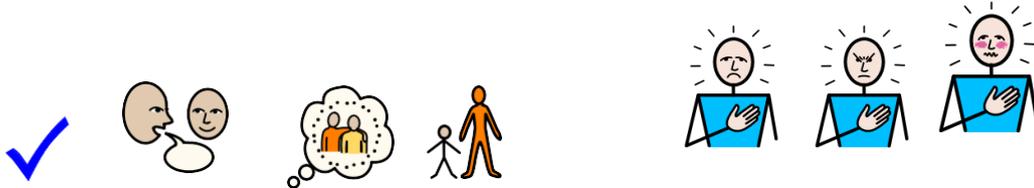
I will ask for help if I'm stuck or not sure.



I will be kind and polite to everyone online.



I will tell a trusted adult if I feel worried, scared or nervous when I am using a device.



I will tell a trusted adult if I feel sad, angry or embarrassed when I am using a device.



I will tell a trusted adult if I feel bad or unsafe when I am using a device.

I know people online sometimes tell lies.



I never have to keep secrets from my trusted adults.

## Parents Acceptable Use Policy

1. I understand KGPS uses technology as part of the daily life of the school when it is appropriate to support teaching & learning and the smooth running of the school, and to help prepare the children and young people in our care for their future lives.
2. I understand that the school takes every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials, including behaviour policies and agreements, physical and technical monitoring, education and support and web filtering. However, the school cannot be held responsible for the nature and content of materials accessed through the internet and mobile technologies, which can sometimes be upsetting.
3. I understand that internet and device use in school, and use of school-owned devices, networks and cloud platforms out of school may be subject to filtering and monitoring. These should be used in the same manner as when in school, **including during any remote learning periods.**
4. I will promote positive online safety and model safe, responsible and positive behaviours in my own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers.
5. The impact of social media use is often felt strongly in schools, which is why we expect certain behaviours from pupils when using social media. I will support the school's social media policy and not encourage my child to join any platform where they are below the minimum age.
6. I will follow the school's digital images and video policy, which outlines when I can capture and/or share images/videos. I will not share images of other people's children on social media and understand that there may be cultural or legal reasons why this would be inappropriate or even dangerous. The school sometimes uses images/video of my child for internal purposes such as recording attainment, but it will only do so publicly if I have given my consent on the relevant form.
7. I understand that for my child to grow up safe online, s/he will need positive input from school and home, so I will talk to my child about online safety.
8. I understand that my child needs a safe and appropriate place to do remote learning if school or bubbles are closed (similar to regular online homework). When on any video calls with school, it would be better not to be in a bedroom but where this is unavoidable, my child will be fully dressed and not in bed, and the camera angle will point away from beds/bedding/personal information etc. Where it is possible to blur or change the background, I will help my child to do

so.

9. If my child has online tuition for catch-up after lockdown or in general, I will undertake necessary checks where I have arranged this privately to ensure they are registered/safe and reliable, and for any tuition remain in the room where possible, and ensure my child knows that tutors should not arrange new sessions or online chats directly with them.
  
10. I understand that whilst home networks are much less secure than school ones, I can apply child safety settings to my home internet. Internet Matters provides guides to help parents do this easily for all the main internet service providers in the UK. There are also child-safe search engines e.g. swiggle.org.uk and YouTube Kids is an alternative to YouTube with age appropriate content.
  
11. I understand and support the commitments made by my child in the Acceptable Use Policy (AUP) which s/he has signed and I understand that s/he will be subject to sanctions if s/he does not follow these rules.
  
12. I can find out more about online safety at KGPS by reading the full Online Safety Policy and can talk to the headteacher if I have any concerns about my child/ren's use of technology, or about that of others in the community, or if I have questions about online safety or technology use in school.

**I/we have read, understood and agreed to this policy**

**Signature/s:** \_\_\_\_\_  
**Name/s of parent / guardian:** \_\_\_\_\_  
**Parent / guardian of:** \_\_\_\_\_  
**Date:** \_\_\_\_\_

## Technician Acceptable Use Policy

The school IT Technician or person with administration rights is placed in an exceptional position of trust. Many of the duties that the Headteacher expects these people to complete could be against the Staff Acceptable User Policy of the school.

This document is not a job description but an addition to the Staff Acceptable User Policy that allows the IT technician to fulfil these duties.

Areas of concern are that:

- Files may be created, imported or processed by staff and pupils and stored on the school's servers or other storage systems (e.g.USB memory sticks, SD cards etc.) that might be of an inappropriate nature to the school setting. Inappropriate use includes any production, processing or transmission of offensive, provocative, racist, unethical, irreligious or anti-social materials in any format. Also included in this area are any materials that are against the rules and conditions of service for the school e.g. material that might bring the establishment into disrepute. Work created during the school's time or on the school's equipment or on one's own equipment but for school work, belongs to the school.
- User accounts will need to be created and serviced meaning that there may be access to these accounts by the IT technician.
- Through work within the school's administration network the IT Technician may be placed in the position of assisting in the processing of confidential information including children's health or MIS data, confidential letters or information from or to senior staff, budgeting plans etc.
- The IT technicians through specific user names and password have control, (sometimes through remote workstations) to the schools network.

Because of these areas of concern the IT Technician should:

- be responsible for monitoring the school's network.
- be given permission to access other user's files.
- protect the users by maintaining a filter for the school.
- monitor the internet use of users within the school.
- be aware of the laws relating to the use of computers especially those around Data Protection, Copyright and those referred to in the school's **online** safety Policy and AUPs.
- make sure that they record all user names and passwords for all the services they access in a place where the senior leaders in the school can access them.
- have their use of the school's network, internet and other aspects of their work open for scrutiny.

To enable them to discharge these duties they should:

- receive training on the sensitive nature of their job especially in relation to Data Protection and the confidentiality of information.
- have an agreed procedure for managing the internet filter. This should include a log of decisions made.
- have an agreed understanding of what is expected of them as far as the regular monitoring of the network system and internet.
- have agreed procedures for reporting incidents.
- log any incidents including minor ones that are quickly resolved.
- be careful to make sure that they are observed when investigating serious incidents to make sure that they are protected against any allegations that could arise (e.g. never open websites that are suspected of having inappropriate material unless others are present).
- have frequent meetings with their line manager to report on any issues or trends.

---

As an IT Technician (or a person who has similar responsibilities) I have read the above document and understand that I will be directed by senior staff to complete work outside of the Staff Acceptable User Policy.

I will report all concerns I have to the headteacher as soon as possible.

Name: \_\_\_\_\_

Signed: \_\_\_\_\_

Senior Member of Staff: \_\_\_\_\_

Date: \_\_\_\_\_

## Occasional Visitors online safety agreement

This list of statements has been developed to use with visitors that are only in school for a one-off occasion such as, a supply teacher that isn't being used regularly by the school, a visiting speaker or students that are helping for single days.

On signing in to KGPS you agree to:



- only log onto the school network with the user name and password provided for you;
- inform the headteacher or their representative if you intend to use the Internet, asking permission before using any kind of social media with the children;
- refrain from any use of your personal mobile phone or other device during the working day;
- not taking any photographs;
- report any suspected misuse or concerns about e-safety whether by pupils or staff, to the headteacher or their representative before leaving the school;
- not taking any information on pupils or staff off site unless specific permission has been given by the headteacher or their representative;

## **Bring Your Own Technology (BYOT)**

The school has decided that for the duration of this policy that no child will bring their own technology into school to use for work.