George Tomlinson Primary School

E – Safety Policy
&
Acceptable Use Policy

Reviewed: February 2021
Ratified by the Governors: March 2021
Due for Revision: February 2022

E-Safety Policy

Contents:

1. Aims and Purpose

New technologies inspire children to be creative, communicate and learn. However, while the internet is a great resource, it is important that children and young people are protected from the risks they may encounter. George Tomlinson Primary School endeavours to highlight benefits and risks of using technology and provides safeguarding and education for users to enable them to control their online experience both inside and outside the classroom.

Our school aims to:

- Have robust processes in place to ensure the online safety of our pupils, staff, volunteers, and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community and its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate
- Continually update and tighten the filtering system in place on all school electronic devices.

This policy applies to all members of our school community (including staff, governors, volunteers, contractors, students/pupils, parents/carers, visitors, and community users) who have access to our digital technology, networks, and systems, whether on-site or remotely, and at any time, or who use technology in their school role.

This policy is based on the Department of Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying advice for Headteachers and school staff
- Searching, screening and confiscation
- Protecting children from radicalisation

The policy reflects the Equality Act 2010 and Education Act 2011, the latter of which has given education professionals stronger powers to tackle cyberbullying by not permitting the use of personal devices in school.

Links to other policies:

- Safeguarding Policy
- Whistleblowing policy
- Behaviour Policy
- Anti-bullying policy
- Guidance on Safer Working Practice
- Staff code of conduct
- Data Protection
- Curriculum Policies (Computing & RHE)
- Remote Learning Policy
- Social Media Policy
- Complaints Policy

2. Roles and Responsibilities

The school community and all members have a duty to behave respectfully online and offline; to use technology for teaching and learning, and to prepare for life after school; and to immediately report any concerns or inappropriate behaviour, to protect pupils, their families and our staff.

School Governors key responsibilities:

- Review this policy's effectiveness
- Ensure an appropriate senior member of staff, from the School Leadership Team (SLT), is appointed to the role of DSL, with lead responsibility for safeguarding and child protection (including online safety)
- Support the school in encouraging parents and the wider community to become engaged in online safety activities
- Incorporate online safety into safeguarding discussions as appropriate
- Ensure that children are taught about safeguarding, including online safety, as part of providing a broad and balanced curriculum

Headteacher key responsibilities:

- Foster a culture of safeguarding where online safety is fully integrated into whole-school safeguarding
- Ensure that policies and procedures are consistently followed by all staff and ensure that staff are aware of reporting procedures in an event of an online safeguarding incident
- Liaise with the DSL on all online-safety issues which might arise and to receive regular updates on school issues and broader policy and practice information
- Ensure the school implements and makes effective use of appropriate ICT systems and services, including school-safe filtering and monitoring, protected email systems and that all technology, including cloud systems, are implemented according to child-safety first principles
- Ensure Governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety
- Ensure the school website meets statutory requirements.

Designated Safeguarding Lead (DSL) Key responsibilities:

- The DSL should take lead responsibility for safeguarding and child protection (including online safety)
- Ensure that all school staff understand this policy and that it is implemented consistently throughout the school
- Ensure all staff are aware of the procedures that need to be followed in the event of an online safety incident, and that these are logged in the same way as any other safeguarding incident
- Work with the SBM, IT Technician, and other staff, as necessary, to address any online safety issues or incidents
- Stay up to date with the latest trends in online safety
- Ensuring that any online safety incidents (including cyber-bullying) are logged on white incident forms/red safeguarding forms as appropriate and dealt with appropriately in line with this policy
- Communicate regularly with SLT and the designated Safeguarding (and online safety) Governor to discuss current issues (anonymised), review incident logs and filtering/change control logs

IT Technician Key responsibilities:

- Implementing appropriate content filtering and monitoring systems, which are updated on a regular basis to keep pupils safe from harmful, inappropriate content, including terrorist and extremist behaviour
- Ensuring that the school's IT systems are secure and protected against viruses and malware, and that safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's IT systems on a weekly basis

- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents (including cyber-bullying) are logged and labelled as such on a white incident form or red safeguarding form as appropriate, and dealt with appropriately in line with this policy

All staff key responsibilities:

- Ensure that all school users understand this policy and ensure that it is implemented consistently throughout the school
- Agree and adhere to the terms of acceptable use of the school's IT systems and internet, ensuring that pupils follow them
- Identify opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum, making the most of unexpected learning opportunities as they arise
- Record online-safety incidents in the same way as any safeguarding incident and report in accordance with school procedures
- Carefully supervise and guide pupils when engaged in learning activities involving online technology (including extra-curricular and extended school activities if relevant), supporting them with search skills, critical thinking (e.g. fake news), age appropriate materials and signposting, and legal issues, such as copyright and data law
- Prepare and check all online sources and resources before using them within the classroom
- Encourage pupils to follow the Acceptable Use Policy (AUP) (see Appendix 8.1 & 8.2), remind them about it and enforcing school sanctions for breaches of the policy
- Notifying the DSL of new trends and issues before they become a problem
- Ensuring that any online safety incidents (including cyber-bullying) are logged on white incident forms/red safeguarding forms as appropriate, and dealt with appropriately in line with this policy.

Pupil key responsibilities:

- Read, understand, sign and adhere to the pupil AUP annually
- Understand the importance of reporting abuse, misuse or access to inappropriate materials
- Know what action to take if they, or someone they know, feel worried or vulnerable when using online technology •
- To understand the importance of adopting safe and responsible behaviours and good online safety practices when using digital technologies outside of school and realise that the school's AUP covers actions out of school, including on social media
- Understand the benefits/opportunities and risks/dangers of the online world and know who to talk to at school or outside school if there are problems

Parents/carers key responsibilities: •

- Read, sign and promote the school's parental AUP and read the pupil AUP and encourage their children to follow it
- Consult with the school if they have any concerns about their children's and others' use of technology
- Promote positive online safety and model safe, responsible, and positive behaviours in their own use of technology, including on social media: not sharing others' 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.

Volunteers and contractors Key responsibilities:

- Read, understand, sign, and adhere to the AUP (where appropriate)
- Report any concerns, no matter how small, to the DSL
- Maintain an awareness of current online safety issues and guidance
- Model safe, responsible, and professional behaviours in their own use of technology

3. Managing e-safety risks

Technical and Infrastructure approaches

- Has the educational filtered secure broadband connectivity through the LGfL and so connects to the 'private' National Education Network
- Uses the LGfL filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc. All changes to the filtering policy is logged and only available to staff with the approved 'web filtering management' status
- Uses USO user-level filtering where relevant, thereby closing down or opening up options appropriate to the age / stage of the students
- Blocks all Chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform
- Has blocked pupil access to music download or shopping sites – except those approved for educational purposes at a regional or national level, such as Audio Network
- Uses security time-outs on Internet access where practicable / useful
- Provides staff with an email account for their professional use, *London Staff mail / LA email* and makes clear personal email should be through a separate account
- Uses teacher 'remote' management control tools for controlling workstations / viewing users / setting-up applications and Internet web sites, where useful
- Has additional local network auditing software installed
- Works in partnership with the LGfL to ensure any concerns about the system are communicated so that systems remain robust and protect students
- Ensures the Systems Administrator / network manager is up-to-date with LGfL services and policies
- Requires the Technical Support Provider to be up-to-date with LGfL services and policies.

The School Website

- The school web site complies with the school's guidelines for publications
- The point of contact on the web site is the school address, telephone number and we use a general email contact address, school@georgetomlinson.waltham.sch.uk . Home information or individual e-mail identities are not be published;
- The Headteacher takes overall editorial responsibility and ensure that content is accurate and appropriate.
- Photographs published on the web do not have full names attached;
- We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website;
- We expect teachers using school approved blogs or wikis to password protect them and run from the school website.

Published Content and The Use of Digital and Video Images

- We gain parental/carer permission for use of digital photographs or video involving their child as part of the school agreement form when their child joins the school
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials / DVDs
- Staff sign the school's AUP and this includes a clause on the use of mobile phones/personal equipment for taking pictures of pupils
- The school blocks/filter access to social networking sites or newsgroups unless there is a specific approved educational purpose

- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location, such as house number, street name or school. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.
- No child should make any digital recording (image or sound) in school using any personal equipment, without express permission from senior staff
- Parents are advised that any images they take in school should not be shared via any public source and should not identify any child by name
- The school reserves the right to instruct parents to take no photographs or video for selected events.

Portable Devices

- All children who bring a mobile phone to school should lodge it with the office whenever they are in school.
- Mobile phones are not to be used in the school; for children who walk home alone then they are to be left at the school office at the beginning of each day. The sending of abusive or inappropriate text messages is forbidden.
- Staff should be aware that technologies such as Ultra-Portable Laptops and mobile phones may access the Internet by bypassing filtering systems and present a new route to undesirable material and communications.
- Staff should not use their personal mobile phones to contact pupils or capture photographs of children. Alternative equipment will be provided by the school.
- Pupils are taught how to protect themselves from being victims of theft and how to report such an event to the correct authority.

Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads, and other tablet devices, where they believe there is a 'good reason' to do so. When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm (for example as a result of a reasonable suspicion that a device contains illegal or undesirable material, including but not exclusive to sexual images, pornography, violence or bullying)
- Disrupt teaching
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the SLT to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation and the school's COVID-19 risk assessment. Any complaints about searching for, or

deleting, inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

Managing Emerging Technologies:

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in the school is allowed
- Games machines including the Sony PlayStation, Microsoft Xbox and others have Internet access, which may not include filtering may not be used in the school
- The school's e-safety strand within the computing curriculum ensures that every pupil is educated about safe and responsible use. Pupils are taught how to control and minimise online risks and how to report a problem through a range of activities that are flexible, relevant and engage pupils' interest.

Social Media

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk School staff should ensure that:
- No reference should be made in social media to students / pupils, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

The school's use of social media for professional purposes will be checked regularly by the Headteacher to ensure compliance.

4. Managing the Network and Equipment

Using the school network, equipment and data safely: General Guidance

The computer system / network is owned by the school and is made available to students to further their education and to staff to enhance their professional activities including teaching, research, administration and management.

The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet or email activity on the network.

To ensure the network is used safely George Tomlinson Primary School:

- Ensures staff read and sign that they have understood the school's e-safety Policy and have signed the AUP. Following this, they are set-up with Internet, email access and network access. Online access to service is through a unique, audited username and password. We also provide a different username to all staff and use the same username and password for pupils for access to our school's network
- We provide pupils with an individual network log-in username

- Make it clear that staff and pupils must always keep their password private, must not share it with others and must not leave it where others can find
- Make clear that no one should log on as another user and makes clear that pupils should never be allowed to log-on or use teacher and staff logins as these have far less security restrictions and inappropriate use could damage files or the network
- Has set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas
- Requires all users to always log off when they have finished working or are leaving the computer unattended
- Where a user finds a logged-on machine, we require them to always log-off and then log-on again as themselves
- Our wireless network has been secured to industry standard Enterprise security level /appropriate standards suitable for educational use.

5. Education and the Curriculum

George Tomlinson as a clear, progressive e-safety education programme throughout all Key Stages. Relationships and Health Education (RHE) was made compulsory in all primary schools in September 2020. Relationships Education puts in place building blocks needed for positive and safe relationships, including with family, friends and online.

Pupils in Key Stage 2 will be taught:

- How to use technology safety, responsibly and respectfully
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

By the end of primary school, pupils will know:

- About different types of bullying (including cyberbullying), the impact of bullying, responsibilities of bystanders (primarily reporting bullying to an adult) and how to get help.
- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships, as to face-to-face relationships, including the importance of respect for others online, including when we are anonymous
- What sorts of boundaries are appropriate in friendships with peers and others (in digital context)
- The rules and principles for keeping safe online, how to recognise risks, harmful content, and contact, and how to report them
- How to critically consider their online friendships and sources of information, including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- How to respond safely and appropriately to adults they may encounter in all contexts, including online, whom they do not know

Remote/Home Learning
In the advent of a pandemic or for other reasons that mean remote learning must take place:

- We will endeavour to ensure that pupils continue to receive a good level of education 'beyond the classroom' by providing a range of resources via our website and learning portals. (See Remote Learning Policy)
- We expect pupils to follow the same principles, as outlined in the school's Acceptable User policy, whilst learning at home.
- If our school chooses to communicate with pupils via Zoom etc then it is important that this is only carried out with the approval of the Headteacher or Senior Leader. Pupils must uphold the same level of behavioural expectations, as they would in a normal classroom setting.
- Any significant behavioural issues occurring on any virtual platform must be recorded, reported and appropriate sanction imposed
- Staff should be mindful that when dealing with any behavioural incidents, online, opportunities to discuss and repair harm will not be the same as if the child or young person was in school. Therefore, it may be necessary to have a discussion with the parents, regardless how minor the incident, to ensure the child is emotionally well supported.

Cyberbullying
To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Classroom staff will discuss cyber-bullying with their tutor groups.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyberbullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors, and volunteers (where appropriate) receive training on cyber-bullying, its impact, and ways to support pupils, as part of safeguarding training.

The school also sends information/leaflets on cyber-bullying to parents, so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school Behaviour Policy. Where illegal, inappropriate, or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained. The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

6. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues, including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required.

The DSL will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills about online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

The schools runs a rolling programme of advice, guidance and training for parents, including:

- Information leaflets; in school newsletters; on the school web site;
- Demonstrations and workshops

More information about safeguarding training is set out in our Child Protection and Safeguarding Policy.

7. How will online concerns and incidents be handled?

Online safety concerns must be handled in the same way as any other safeguarding concern. Safeguarding is often referred to as a jigsaw puzzle, so all stakeholders should talk to the DSL if they are concerned about a pupil, to contribute to the overall picture or highlight what might not yet appear to be a problem

Support staff will often have a unique insight and opportunity to find out about issues first in the playground, corridors, toilets, and other communal areas outside the classroom (particularly relating to bullying and sexual harassment and violence).

School procedures for dealing with online safety will be mostly detailed in the following policies:

- Safeguarding and Child Protection Policy
- Anti-Bullying Policy
- Behaviour Policy
- Acceptable Use Policy (AUP)
- Data Protection Policy, agreements, and other documentation (e.g., consent forms for data sharing, image use, etc)

George Tomlinson Primary School commits to take all reasonable precautions to ensure online safety, but recognises that incidents will occur both inside and outside school (and that those from outside school will continue to impact on pupils when they come into school).

George Tomlinson fosters a 'No Blame' environment that encourages pupils to tell a teacher / responsible adult immediately if they encounter any material that makes them feel uncomfortable. All members of the school are encouraged to report issues swiftly to allow us to deal with them quickly and sensitively through the school's escalation processes. Any suspected online risk or infringement should be reported to the DSL on the same day – where clearly urgent, it will be reported by the end of the lesson. Any concern/allegation about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher, in which case the complaint is referred to the Chair of Governors and the LADO (Local Authority's Designated Officer). Staff may also use the NSPCC Whistleblowing Helpline: 0800 0280285 The school will actively seek support from other agencies as needed e.g. the UK Safer Internet Centre's Professionals' Online Safety Helpline, NCA CEOP, the Prevent Officer, the police, the Internet Watch Foundation (IWF). We will inform parents/carers of online-safety incidents involving their children, and the police where staff or pupils engage in, or are subject to, behaviour which we consider is particularly disturbing or breaks the law.

8. Appendices: Acceptable Use Policy/Agreement

APPENDIX 8.1

<table>
<tr><th colspan="2">Pupil and Parent/Carer Acceptable Use Agreement: EYFS and KS1</th></tr>
<tr><td colspan="2">Name of pupil:</td></tr>
<tr><td colspan="2">This is how we stay safe when we use computers:
• I will ask a teacher or suitable adult if I want to use the computers/tablets
• I will only use activities that a teacher or suitable adult has told or allowed me to use
• I will take care of computers/tablets and other equipment
• I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong
• I will tell a teacher or suitable adult if I see something that upsets me on the screen
• I know that if I break the rules, I might not be allowed to use a computer/tablet
• I agree that the school will monitor the websites I visit and that there will be consequences if I do not follow the rules.</td></tr>
<tr><td>Signed (pupil):</td><td>Date:</td></tr>
<tr><td colspan="2">Parent/carer agreement:
I agree that my child can use the school’s ICT systems and internet when appropriately supervised by a member of school staff.
I agree to the conditions set out above for pupils using the school’s ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.</td></tr>
<tr><td>Signed (parent/carer):</td><td>Date:</td></tr>
</table>

APPENDIX 8.2

Pupil and Parent/Carer Acceptable Use Agreement: KS2

Name of pupil:

I will read and follow the rules in the Acceptable Use Agreement Policy

When I use the school's ICT systems (e.g. computers) and get onto the internet in school, I will:

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

I will not:

- Access any inappropriate websites, including social networking sites, chat rooms and gaming sites, unless my teacher has expressly allowed this as part of a learning activity
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails

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

- Log into the school's network using someone else's details
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision
- I will not use it during lessons, tutor group time, clubs or other activities organised by the school without a teacher's permission
- I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online

I agree that the school will monitor the websites I visit and that there will be consequences if I do not follow the rules.

Signed (pupil):	**Date:**

Parent/carer agreement:

I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff.

I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Signed (parent/carer):	**Date:**

APPENDIX 8.3

Pupil and Parent/Carer Acceptable Use Agreement Template: Staff, Governors, Volunteers and Visitors

Name of staff member/governor/volunteer/visitor:

When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), 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
- Take photographs of pupils without checking with teachers first
- I will not take any photographs without all involved being aware that images are being captured and the purpose for which they are being captured.
- Share confidential information about the school, its pupils or staff, or other members of the community
- Access, modify or share data I am not authorised to access, modify or share
- Promote private businesses, unless that business is directly related to the school

- I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.
- I agree 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.
- All images of pupils will be captured using school owned cameras and all data should be kept in school and transferred electronically to school servers.
- Before taking a school owned digital image capture device off site, I will ensure that any images already held on that device are backed up in school and will delete any images that clearly identify children or staff by name.
- During off-site visits, I will ensure that any digital image capture device is held securely by a member of staff.
- I will ensure that any children or staff are made aware of any photographs being taken and are given the opportunity to view these images on demand.
- I will let the Designated Safeguarding Lead (DSL) and ICT manager know if a pupil informs me that 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:**
