St. James CE Primary School

St. James CE Primary School

Online Safety Policy
and Acceptable Use Agreement

Flourish
Respect   Courage
Friendship Develop
StrongGrowth
Community   StJames'   Strive
God Trust Kindness
Perseverance
Freedom Unique
DeepRoots Positivity
WholeChild
Responsibility

St James' CE Primary School is committed to the safeguarding of our pupils and staff.

Statement of Vision and Values

In consultation with pupils, parents, governors, community members and staff our vision and values were generated based on our inspiration from the Parable of the Sower and how this links to our children and their journey with us.

> ### Our School Vision:
> Within our community we strive to develop deep roots, strong growth and freedom to flourish as a unique and whole child of God.

Matthew 13 - The Parable of the Sower – '… but the seed falling on good soil refers to someone who hears the word and understands it. …….produces a crop, yielding a hundred, sixty or thirty times what was sown."

Values

We decided at St James CE Primary School that Kindness and Respect are values which we feel underpin our vision and are incorporated in all we do and say – so therefore these two values will be taught alongside all the other six values we have chosen.

½ termly focus	Value
Autumn 1	Responsibility
Autumn 2	Friendship
Spring 1	Perseverance
Spring 2	Trust
Summer 1	Courage
Summer 2	Positivity

St James' CE Primary School is committed to the safeguarding of our pupils and staff.

Online Safety Policy

St. James CE Primary School is proud to have children from diverse cultural backgrounds and a variety of ethnic groups. We value the positive contributions that all children bring to the school. The school's motto, 'Learning, growing and flourishing together' is embedded in the teaching and learning in the school. This is aligned to our Christian ethos and high expectations from both children and staff. Our online safety policy also reflects our school values which include respect, responsibility, trust and courage.

Our IT & Computing Vision is:

We empower our children to learn, create and work, using concepts and technology. We encourage all children to be competent digital experts with an understanding of the importance of being safe online for themselves and others.

This policy should be read in conjunction with our data protection, behaviour and whistleblowing policies.

Introduction

IT and Computing in the 21st Century is seen as a critical resource to support learning and teaching, as well as playing what is now regarded as an essential role in everyday lives of children, young people, and adults. Consequently, schools need to ensure children are properly equipped with the skills to access IT and promote life-long learning and future economic well-being.

IT and Computing covers a wide range of resources including web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of computing within our society. Currently the internet software children and young people are using, both inside and outside of the classroom include:

● Websites

● Learning Platforms and Virtual Learning Environments

● Email and Instant Messaging

● Chat Rooms and Social Networking

● Blogs and Wikis

● Podcasting

● Video Broadcasting

● Gaming

● Mobile/Smart phones with text, video and/or web functionality

● Other mobile devices with web functionality

● QR Codes

Whilst exciting and beneficial, both in and out of the context of education, much IT and computing, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these internet technologies.

At St. James CE Primary School, we understand the responsibility to educate our pupils in Online Safety issues; teaching children the appropriate behaviours and critical thinking, to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

St James' CE Primary School is committed to the safeguarding of our pupils and staff.

This policy is inclusive of both fixed and mobile internet; technologies provided by the school; (such as PCs, laptops, netbooks, IPads, iPod, webcams, whiteboards, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobiles phones, camera phones and portable media players, etc). For additional information please refer to our GDPR Policy.

Legislation and guidance

This policy is based on the Department for Education's (DfE's) 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

[Relationships and sex education

Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

Roles and Responsibilities

As Online Safety is an important aspect of strategic leadership within the school, the Head of School and Governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. All staff share responsibility for e-safety, however, our designated safeguarding officers have an extra responsibility within this area based on their role. All members of the school community have been made aware of who holds these posts. It is the role of the Safeguarding officers to keep up-to-date of current issues and guidance through organisations such Enfield LA, LGFL, CEOP (Child Exploitation and Online Protection) and Childnet.

The Head of school, ICT/ computing lead alongside our external computing support team will ensure that Governors have an understanding of the issues at our school in relation to local and national guidelines and advice and that they remain updated.

Writing and reviewing the Online Safety policy

This policy, supported by the school's Acceptable Use Agreement for staff, governors, visitors, and pupils, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies including those for ICT, home-school agreements, behaviour, Health and Safety, Child Protection, and PSHE/SMSC policies including Anti-bullying.

The Online Safety policy and its implementation will be reviewed annually.

Online Safety skills development for staff

- Staff receive regular information and training on Online Safety issues through our consultant at staff meetings and by the Executive Headteacher/Head of School in staff briefings. They also receive annual INSET Training run by ECP Ltd.

St James' CE Primary School is committed to the safeguarding of our pupils and staff.

- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of Online Safety and know the protocol to follow in the event of misuse of technology by any member of the school community.
- New staff are talked through the policy and asked to sign the school's Acceptable Use Agreement as part of their induction.
- All staff will deliver Online Safety lessons as part of the IT and Computing curriculum as set out in the Rising Stars Computing curriculum.
- All staff will refer to Online Safety at the start of any lesson involving using new technologies.

Online Safety information for parents/carers/visitors

- Parents/carers/visitors are asked to read through and sign the Acceptable Use Agreement on behalf of their child when their child starts school.
- Parents/carers/visitors are required to decide as to whether they consent to images of their child being taken/used on the school website, or on the Virtual Learning Platform -Google Classroom. It is the responsibility of parents/carers to inform the school if their decision changes.
- The school website and Google Classroom contain useful information and links to sites like 'ThinkUknow', Childline, National Online Safety and Child Net.
- The school will send out relevant Online Safety information through newsletters, the school website, Google Classroom and the school brochure.

Community use of the Internet
- External organisations using the school's IT facilities must adhere to the Online Safety policy.

More recent concerns:

Radicalisation
As a school we are aware that during the teaching of Computing or use of the internet, a teacher or assistant, may become concerned that a child is at risk of being radicalised, possibly through what they say, discuss, write or draw. The adult has a responsibility to follow our safeguarding and reporting procedures. Please refer to our Safeguarding Policy.

Sexting
We are aware that sexting (the sending of indecent images to a friend) has become more prolific and could become an issue with primary aged children. We will make explicit reference to personal safety and decency when using mobile phones and cameras and ensure our older children are aware of it being illegal and inappropriate.

Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

St James' CE Primary School recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create

St James' CE Primary School is committed to the safeguarding of our pupils and staff.

images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

St James' CE Primary School will treat any use of AI to bully pupils in line with our [anti-bullying/behaviour] policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the St James' CE Primary School

Cyber-bullying

Definition: Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

Preventing and addressing cyber-bullying

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. Class teachers will discuss cyber-bullying with their class within computing and the PSHE sessions. Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. 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 provides information on cyber-bullying to parents/carers so 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 report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

2. **Teaching and Learning**

Internet use will enhance learning

- The school will provide opportunities within a range of curriculum areas to teach e-Safety.

- Educating pupils on the dangers of technologies that may be encountered outside school is done informally when opportunities arise and as part of the Online Safety curriculum.

- Pupils should be made constantly aware of the impact of online bullying and know how to seek help if these issues affect them. Pupils must also be made aware of where to seek advice or help if they experience problems when using the Internet and related technologies, i.e. parent/carer, teacher/trusted member of staff, or an organisation such as Childline/CEOP.

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.

St James' CE Primary School is committed to the safeguarding of our pupils and staff.

- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval, and evaluation.

Pupils will be taught how to evaluate Internet content

- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

3.   **Managing Internet Access**

Information system security

The Internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas, and publish material. This makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people when not used appropriately.

- School IT systems capacity and security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed with Enfield LA, our IT support and Consultant.

E-mail

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail (blow the whistle).
- Pupils must not reveal personal details of themselves or others in e-mail communication or arrange to meet anyone without specific permission.
- The forwarding of chain letters is not permitted.

Published content and the school web site

The contact details on the Website should be the school address, e-mail and telephone number. Staff or pupils' personal information will **not** be published. The Head Teacher and School Office Manager will take overall editorial responsibility and ensure that content is accurate and appropriate. All office staff must check and agree content before posting.

Publishing pupil's images and work

- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website or Google Classroom. This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue.
- Parents/carers may withdraw permission, in writing, at any time.
- Photographs that include pupils will be selected carefully and **will not** enable individual pupils to be identified by their full name inline with our GDPR policy.

St James' CE Primary School is committed to the safeguarding of our pupils and staff.

- Pupils' full names will not be used in association with photographs. Children's first names will only be used when celebrating achievements.
- A pupil's work can only be published by outside agencies with the permission of the pupil and parents/carers.

Photographs taken by parents/carers for personal use

In the event of parents/carers wanting to take photographs for their own personal use, the school will demonstrate our protective ethos by announcing that photographs taken are for private retention and not for publication in any manner, including use on personal websites and social media e.g. School performances and assemblies etc. Parents/ carers will take full responsibility if there is any infringement of this rule.

Social networking and personal publishing

- The school will block / filter access to social networking sites.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils. However, we accept that some pupils will still use them; they will be advised never to give out personal details of any kind, which may identify them, our school or their location.
- Pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- Our pupils are asked to report any incidents of bullying to the school.
- School staff are not permitted to add children as 'friends' if they use these sites.
- PSCOs/local safe-guarding board will come into school regularly to speak to KS2 children about the dangers of these sites and appropriate safety procedures (e.g. not wearing school uniform)
- Adults/Children must not put school photos up on these sites, or other photos of themselves or others in school uniform, which makes them easily identifiable.

Managing filtering

- The school will work with the LA, DfE and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- If pupils discover an unsuitable site, it must be reported to the Class Teacher immediately.
- If staff discover unsuitable sites, they must report it to the Computing Lead, Head Teacher or Deputy Head. The computing lead will then work with our IT support to ensure the site is blocked.

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Pupils are not allowed to bring personal mobile devices/phones to school. Where an exception is agreed in writing any phones that are brought to school must be switched off and given to the school office and kept there until the end of the day.
- Any phones brought into school without permission, or sounding in school, will be confiscated and must be collected by the child's parents.
- The sending of abusive or inappropriate text messages outside school is forbidden. Any abusive or offensive messages must be kept as evidence and reported to the class teacher (in the case of children) or Head Teacher (in the case of staff).

St James' CE Primary School is committed to the safeguarding of our pupils and staff.

- For the recording of children's activities, Staff should use school IPads for photos and videos inside and outside school. Staff are not permitted to use their personal mobile phones for photos and videos of children

Managing video-conferencing

- Videoconferencing and skyping should use the school network.
- All Online Safety procedures must be adhered to, to protect children's identities.
- Videoconferencing will be appropriately supervised.

Protecting personal data

The school will collect personal information about pupils and staff fairly and will let them know how the school and Enfield LA will use it. The school will use information about pupils to further curriculum, professional and managerial activities in accordance with the business of the school and will contact the parents or guardians, if it is necessary, to pass information beyond the school or Enfield LA. For other members of the community the school will tell parents/carers/staff in advance if it is necessary to pass the information on to anyone else other than the school and Enfield LA.

The school will hold personal information on its systems for as long as staff/pupils remain a member of the school community and remove it in the event of their leaving or until it is no longer required for the legitimate function of the school. We will ensure that all personal information supplied is held securely, in accordance with the policies and practices of Enfield LA and as defined by the Data Protection Act 2018 as well as the school's GDPR Policy.

Staff/Parents/Carers have the right to view the personal information that the school holds about them and to have any inaccuracies corrected.

Accessing School Information from Home.

Teaching staff have access to Pupil Tracker, our google classroom, google drive. In addition, leaders have access to the school data system. All staff must adhere to online safety guidelines to ensure the integrity of the school and safety of the school community when accessing school information from home. Such information must only be accessed through school provided surface pros where possible or private computers and not public ones (e.g. library computers).

Policy Decisions

Authorising Internet access

- Pupil instruction in responsible and safe use should precede any Internet access and all pupils must sign up to the Acceptable Use Agreement for pupils and abide by the school's Online Safety rules. These Online Safety rules will also be displayed clearly in each teaching area.

- Access to the Internet will be by directly supervised access to specific, approved on-line materials.

- All parents/carers will be asked to sign the Acceptable Use Agreement for pupils giving consent for their child to use the Internet in school by following the school's Online Safety rules and within the constraints detailed in the school's Online Safety policy.

- All staff must read and agree in writing to adhere to the Acceptable Use Agreement for Staff before using any school ICT resource.

St James' CE Primary School is committed to the safeguarding of our pupils and staff.

Password Security

- Adult users are provided with an individual network, email and google classroom login username and password, which is changed every 90 days.
- All pupils are provided with an individual login for our (educational learning platform) and Google Classroom, TTRS (Timestable Rockstars) & Maths Shed username and passwords.
- Children are taught to logout when they have finished their access as part of security.
- Pupils are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others.
- Staff are aware of their individual responsibilities to protect the security and confidentiality of the school network, MIS systems.

Assessing risks

The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Enfield LA can accept liability for the material accessed, or any consequences of Internet access. The school will audit IT provision to establish if the Online Safety policy is adequate and that its implementation is effective.

How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on (behaviour and ICT and internet acceptable use). The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the [staff disciplinary procedures / staff code of conduct]. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

Handling Online Safety complaints

- Complaints of Internet misuse will be dealt with by a member of the Strategic Leadership Team and reported to the Online Safety Leader.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the Online Safety Leader and recorded in the Online Safety Logbook which is situated in the school Office.
- Any complaint about staff misuse must be referred to the Executive Headteacher/Head of School (see Whistle blowing Policy).
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints' procedure.

St James' CE Primary School is committed to the safeguarding of our pupils and staff.

Communications Policy

Introducing the Online Safety policy to pupils

- Online Safety rules will be displayed and discussed with the pupils throughout the year. Specific lessons will be taught by class teachers in accordance with our Online Safety curriculum. Children will be reminded at the start of any activity using the internet.
- Pupils will be informed that network and Internet use will be monitored.
- Online Safety buttons will be discussed, and their use encouraged when inappropriate material is displayed (for children using sites at home).

Staff and the Online Safety policy

- All staff will be given the School Online Safety policy and its importance explained.
- Any information downloaded must be respectful of copyright, property rights and privacy.
- Staff should be aware that Internet traffic could be monitored and traced to the individual user. Discretion and professional conduct is essential.
- A laptop/iPad issued to a member of staff remains the property of the school. Users of such equipment should therefore adhere to school policy regarding appropriate use with regards to Internet access, data protection and use of software, both in and out of school.

The Learning Platform – currently Google Classroom

- All staff will be trained and given advice on how to use Google Classroom effectively.

- Parents will be informed about what Google Classroom is and how it can enhance the learning of each child. All children will be given training on how to effectively use Google Classroom.

- All children will be given a username and password to access secure resources and facilities through DB Primary. Children will be taught to keep this secure.

- If a child sends an inappropriate message through the schools Google Classroom, the recipient should keep this as evidence and this should be reported to the class teacher, who will in turn report this to the Executive Head Teacher/Head of School and ICT & Computing Lead.

- Children will be allowed to upload photographs of groups or group activities onto the class page.

- Class teachers will monitor the use of Google Classroom. Any misuse of Google Classroom will be reported to the Executive Head Teacher/Head of School – and sanctions imposed.

7. Monitoring and review

This policy is implemented on a day-to-day basis by all school staff and is monitored by the Online Safety Leader.

This policy is the Governors' responsibility, and they will review its effectiveness biannually. They will do this during reviews conducted between the ICT & Computing Subject Leader, Designated Child Protection Officer, and Governor with responsibility for Safeguarding Children. Ongoing incidents will be reported to the full governing body.

The Online Safety policy will be revised by the Online Safety Leader.

This policy was updated in February 2024   Date for review: February 2025

St James' CE Primary School is committed to the safeguarding of our pupils and staff.

St James' CE Primary School is committed to the safeguarding of our pupils and staff.

PUPIL GUIDELINES FOR SAFE Internet/
Google Classroom

I will only use the Internet when there is a teacher present.

I understand that Google Classroom and the Internet are to be used to support my learning and facilitate appropriate discussions with my peers and teachers only

I will always ask for permission before accessing the Internet/ Google Classroom

I will only use my own usernames and passwords to log on to the system/ Doodle/ Google Classroom and keep them secret.

I will not access other people's files.

I will only message people I know, or that my teacher has approved, and ensure that the messages that I send will be polite and responsible.

I understand that the use of abusive language, swearing or aggressive behaviour is not allowed when using Google Classroom.

I will not give personal details (like my home address, telephone or mobile number), or the personal details of any other person to anyone or arrange to meet someone unless my parent/carer or teacher has given me permission.

I will only download, use or upload material when I have been given the owner's permission.

I will not upload individual images of myself or other members of the school community

I will only view, download, store, or upload material that is lawful, and appropriate for other users. If I am not sure about this, or come across any potentially offensive materials, I will inform my class teacher straight away.

I will avoid any acts of vandalism. This includes, but is not limited to, uploading, or creating computer viruses and mischievously deleting or altering data from its place of storage.

I will always quote the source of any information gained from the Internet i.e. the web address, in the documents I produce.

I will use the Internet for research and school purposes only.

I will not bring in memory sticks from home to use in school unless I have been given permission by my class teacher.

I understand that the school will check my computer files/ Google Classroom and will monitor the Internet sites that I visit.

I understand that if I don't follow these rules, my access to the school computer system/Internet/ Google Classroom may be suspended, and my parents/carers will be informed.

St. James CE Primary School

Pupils' Acceptable Use Agreement

I have read and understood the **Guidelines for Safe Internet/Timestable Rock stars, Mathshed & Google Classroom and agree to adhere to them.**

Pupil's Name		Class Teacher	
As a school user of the internet, I agree to follow the school rules on its use. I will use the network in a responsible way and observe all the restrictions explained to me by my school. I understand that if I break any of the rules, I will be banned from using the school IT equipment for a period of time and given a reminder about my future use. Misuse of the school Google Classroom/TTRS/Mathshed will result in my access being blocked.			
Pupil Name (print)			
Pupil Signature		Date	

Parent's Name	
As the parent or legal guardian of the pupil above, I give permission for my son or daughter to use the internet, including Google Classroom/TTRS/Mathshed. I understand that pupils will be held accountable for their own actions. I also understand that some of the materials on the Internet may be unsuitable and I accept responsibility for setting standards for my daughter or son to follow when selecting, sharing and exploring information.	
Parent's Name (print)	
Parent's Signature		Date	

This form must be returned to your child's class teacher

St James' CE Primary School is committed to the safeguarding of our pupils and staff.

St. James CE Primary School - Staff Acceptable Use Agreement

The computer system is owned by the school and is made available to staff to enhance their professional activities including teaching, research, administration and management. The school's Internet Access Policy has been drawn up to protect all parties – the children, the staff and the school. The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet sites visited. Staff requesting internet access should sign a copy of this Acceptable Internet Use Statement and return it to the Executive Head Teacher/ Head of School for approval.

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 Office Staff first to ensure that the child has consent to be photographed
- Take photographs of any pupil using a personal device
- 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 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.
- I will let the designated safeguarding lead (DSL) and computing lead 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):

Name		
Date		Signed