Online Safety Policy



Autumn 2020

**Contents**

1. Rationale
2. Aims
3. Legislation and guidance
4. Roles and Responsibilities
5. Educating pupils about online safety
6. Educating parents about online safety
7. Cyber-bullying
8. Acceptable use of the internet in school
9. Pupils using mobile devices in school

10.Staff using work devices outside school

1. School response to issues of misuse

12.Training

13. Monitoring arrangements

14. EYFS

15. Review

Appendix 1: Acceptable use policy for pupils

Appendix 2: Acceptable use agreement (pupils and parents/carers)

Appendix 3: Acceptable use policy for staff/governors

Appendix 4: Acceptable use agreement (staff, governors, volunteers and visitors)

Appendix 5: Online safety training needs – Self audit for staff

Appendix 6: Futures Cloud Technology Misuse Log

1. **Rationale**

Online safety knowledge ensures that pupils become aware of and vigilant around online and digital misuse at a level suitable for the future workplace and as active participants in a digital world.

1. **Aims**

Online safety in St Giles’ and St George’s Academy aims to give our pupils the knowledge to use technology, that allows access online, safely and to give them the knowledge of what to do if they see misuse of the online world.

We aim to ensure that we:

• have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors.

• deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology.

• establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

1. **Legislation and guidance**

This policy is based on the Department for Education’s statutory safeguarding guidance, [Keeping Children Safe in Education](https://www.gov.uk/government/publications/keeping-children-safe-in-education--2), and its advice for schools on [preventing and tackling bullying](https://www.gov.uk/government/publications/preventing-and-tackling-bullying) and [searching, screening and confiscation](https://www.gov.uk/government/publications/searching-screening-and-confiscation). It also refers to the Department’s guidance on [protecting children from radicalisation](https://www.gov.uk/government/publications/protecting-children-from-radicalisation-the-prevent-duty).

It reflects existing legislation, including but not limited to the [Education Act 1996](https://www.legislation.gov.uk/ukpga/1996/56/contents) (as amended), the [Education and Inspections Act 2006](https://www.legislation.gov.uk/ukpga/2006/40/contents) and the [Equality Act 2010](https://www.legislation.gov.uk/ukpga/2010/15/contents). In addition, it reflects the [Education Act 2011](http://www.legislation.gov.uk/ukpga/2011/21/contents/enacted), 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](https://www.gov.uk/government/publications/national-curriculum-in-england-computing-programmes-of-study).

This policy complies with our funding agreement and articles of association.

1. **Roles and Responsibilities**

**4.1 The governing board**

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governor who oversees online safety is *Mrs Amanda Roache*

All governors will:

* Ensure that they have read and understand this policy

- Agree and adhere to the terms on acceptable use of the school’s ICT systems and the internet (appendix 2)

**4.2 The Headteacher**

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

**4.3 The designated safeguarding lead**

Details of the school’s designated safeguarding lead (DSL) and deputies are set out in our child protection and safeguarding policy.

The DSL takes lead responsibility for online safety in school, in particular:

* Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
* Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
* Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
* Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
* Updating and delivering staff training on online safety (appendix 3 contains a self-audit for staff on online safety training needs)
* Liaising with other agencies and/or external services if necessary
* Providing regular reports on online safety in school to the headteacher and/or governing board

This list is not intended to be exhaustive.

**4.4 The ICT Technician**

The ICT technician is responsible for:

* Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
* Ensuring that the school’s ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
* Conducting a full security check and monitoring the school’s ICT 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 are logged and dealt with appropriately in line with this policy
* Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

**4.5 All staff and volunteers**

All staff, including contractors and agency staff, and volunteers are responsible for:

Maintaining an understanding of this policy

Implementing this policy consistently

Agreeing and adhering to the terms on acceptable use of the school’s ICT systems and the internet (appendix 2), and ensuring that pupils follow the school’s terms on acceptable use (appendix 1)

Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy

Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

**4.6 Parents**

Parents are expected to:

Notify a member of staff or the headteacher of any concerns or queries regarding this policy

Ensure their child has read, understood and agreed to the terms on acceptable use of the school’s ICT systems and internet (appendix 1)

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

What are the issues?, UK Safer Internet Centre: <https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues>

Hot topics, Childnet International: <http://www.childnet.com/parents-and-carers/hot-topics>

Parent factsheet, Childnet International: <http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf>

**4.7 Visitors and members of the community**

Visitors and members of the community who use the school’s ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 2).

1. **Educating pupils about online safety**

Pupils will be taught about online safety as part of the curriculum using **Common Sense Media** planning from Y1-6 for stand alone sessions once every half term. EYFS will follow schemes from Twinkl and Childnet for age appropriate online safety information.

In **Key Stage 1**, pupils will be taught to:

Use technology safely and respectfully, keeping personal information private

Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage 2** will be taught to:

Use technology safely, respectfully and responsibly

Recognise acceptable and unacceptable behaviour

Identify a range of ways to report concerns about content and contact

How to report a range of concerns

The safe use of social media and the internet will also be covered in other subjects where relevant.

The school will use assemblies to raise pupils’ awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

Through Computing lessons, assemblies and PSHE, children will be taught the **SMART** rules:

|  |  |
| --- | --- |
| **S**AFE | Keep safe by being careful not to give out personal information online. |
| **M**EETING | Never agree to meet anyone that you chat to on the internet; they may not be who you think they are. You can’t be sure who you are talking to on the Internet. |
| **A**CCEPTING | Do not accept unusual e-mails. They may be trying to tempt you into opening them. They could contain viruses that can damage your computer. If this happens to you, tell an adult. |
| **R**ELIABLE | Information on the Internet may not be true – anyone can upload material to the internet. Always double check any information on a more reliable website |
| **T**ELL | If anything makes you feel worried tell your parents, teachers or an adult that you trust. They can help you to report it to the right place Or call a helpline like Childline on 0800 1111 in confidence. |

1. **Educating parents about online safety**

The school will raise parents’ awareness of internet safety in letters or other communications home, and in information via our website ‘Online Safety’ page and Facebook feed. This policy will also be shared with parents.

Online safety will also be covered during parents’ evenings.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

1. **Cyber-bullying**

**7.1 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 one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

**7.2 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 pupils, and the issue will be addressed in assemblies.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. 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 endeavors 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.

**7.3 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, and/or

Disrupt teaching, and/or

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 senior leadership team 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](https://www.gov.uk/government/publications/searching-screening-and-confiscation).

Any complaints about searching for or deleting inappropriate images or files on pupils’ electronic devices will be dealt with through the school complaints procedure.

1. **Acceptable use of the internet in school**

Use of the school’s internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual’s role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above and Appendix 1, 2, 3, and 4.

* 1. **Acceptable use Staff and Governors (See appendix 3 and 4)**

All members of staff have a responsibility to use the school’s computer system in a professional, lawful, and ethical manner. Our AUP must be fully complied with at all times. All users of the school network should note that it is monitored on a regular basis. Any person who is found to have misused the school system or not followed our AUP could face the following consequences:

* Temporary or permanent withdrawal from the school system
* Suspension or exclusion from the school
* Disciplinary action
* In the most serious cases legal action may also be taken.

All staff and governors who will be using the online systems in school must read Appendix 3 and read and sign Appendix 4.

* 1. **Acceptable use Pupils (See Appendix 1 and 2)**

All pupils and parents are required to sign an agreement regarding the acceptable use of the school’s ICT systems and the internet (appendices 1 and 2).

* 1. **Volunteers and Visitors**

Visitors and volunteers will be expected to read and agree to the school’s terms on acceptable use if relevant to their role (Appendix 3 and 4).

1. **Pupils using mobile devices in school**

Only year 5 and 6 children are allowed to bring their mobile phone into school but must hand it to the teacher at the beginning of the school day for safekeeping. Pupils will not have access to the device throughout the day. The pupil can then collect the device at the end of the school day.

1. **Staff using work devices outside school**

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school’s terms of acceptable use, as set out in appendix 2.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted.

If staff have any concerns over the security of their device, they must seek advice from the ICT manager/Technician. Work devices must be used solely for work activities.

1. **School response to issues of misuse**

Where a pupil misuses the school’s ICT systems or internet, we will follow the procedures set out in the behaviour policy. 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. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

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

1. **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 (for example through emails, e-bulletins and staff meetings).

The DSL and deputies 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 on the subject of 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.

More information about safeguarding training is set out in our child protection and safeguarding policy.

1. **Monitoring arrangements**

Should a member of staff have an online safety concern about a child or member of staff, they should use the MyConcern reporting system to report the concern, ensuring to select the Online Safety lead to send the concern to.

The online safety lead will monitor the use of laptops and computers in school through FuturesCloud Monitoring system every week. Any concerns will be logged using Appendix 4 and if appropriate on MyConcern. It is the adult in the rooms responsibility to monitor the pupils use of iPads.

If a volunteer, lunchtime or anyone who does not have a MyConcern account, has a concern about a child and their online safety, they should report this concern to the DSL or headteacher in as much detail as possible,

1. **EYFS**

Mobile devices are not allowed in EYFS for any reason, staff must lock their phone in the staff room lockers. Office staff will ask for visitors to relinquish their mobile phone at the front door if visiting EYFS.

1. **Review**

This policy will be reviewed by the Computing and Online Safety Leader in September 2021 in conjunction with the headteacher. At every review, the policy will be shared with the governing board.

**Appendix 1: Acceptable use policy for pupils**

Using the Internet to Enhance Learning

Access to the internet is a planned part of the curriculum that will enrich and extend learning activities and is integrated into schemes of work. As in other areas of their work, we recognise that pupils learn most effectively when they are given clear objectives for Internet use.

Different ways of accessing information from the Internet will be used depending on the nature of the material being access and the age of the pupils:

* Access to the Internet may be by teacher demonstration.
* Pupils may be given a suitable web site to access using a link from in a teacher-prepared Word document.
* Pupils may be provided with lists of relevant and suitable websites which they may access.
* Older pupils may be allowed to undertake their own Internet search, pupils will be expected to observe the Rules of Responsible Internet use and will be informed that checks can and will be made on files and the sites they access.

Pupils accessing the internet will be supervised by an adult, normally their teacher, at all times. They will only be allowed to use the Internet once they have been taught the Rules of Responsible Internet Use and the reasons for these rules. Teachers will endeavour to ensure that these rules remain uppermost in the children’s minds as they monitor the children using the Internet.

Using Information from the Internet

In order to use information from the Internet effectively, it is important for pupils to develop an understanding of the nature of the Internet and the information available on it:

* Pupils will be taught to expect a wider range of content, both in level and in audience, than is found in the school library or on television.
* Teachers will ensure that pupils are aware of the need to validate information whenever possible before accepting it as true, and understand that this is even more important when considering information from the Internet.
* When copying materials from the Web, pupils will be taught to observe copyright;
* Pupils will be made aware that the writer of an e-mail or the author of a web page may not be the person claimed.

Using E-mail

It is important that communications are properly managed to ensure appropriate educational use and that the good name of the school is maintained. Therefore:

* Incoming and outgoing e-mail is accessed via webmail and not downloaded onto school computers.
* Pupils will only be allowed to use the e-mail facility once they have been taught the Rules of Responsible Internet Use and the reasons for these rules.
* Teachers will endeavour to ensure that these rules remain uppermost in the children’s minds as they monitor children using e-mail.
* Children will have the e-mail messages they compose checked by a member of staff before sending.
* Incoming e-mail to class e-mail addresses will not be regarded as private.
* Pupils will not be permitted to use e-mail at school to arrange to meet someone outside school hours.
* The forwarding of chain letters will not be permitted.

Maintaining the Security of the School ICT Network

Connection to the Internet significantly increases the risk that a computer or a computer network may be compromised or accessed by unauthorised persons. Users should not expect that files stored on servers or storage media are always private.

Ensuring Internet Access is Appropriate and Safe

The internet is freely available to any person wishing to send e-mail or publish a web site. In common with other media such as magazines, books and video, some material available on the Internet is unsuitable for pupils. Pupils in school are unlikely to see inappropriate content in books due to selection by publisher and teacher and the school will take every practical measure to ensure that children do not encounter upsetting, offensive or otherwise inappropriate material on the Internet. The following key measures have been adopted to help ensure that our pupils are not exposed to unsuitable material:

* Our Rules and Responsible Internet Use are printed in the Children’s planners and signed by parents and children each year;
* Children using the internet will normally be working during lesson time and will be supervised by an adult at all times;
* Staff will check that the sites pre-selected for pupil use are appropriate to the age of the pupils;
* Staff will be particularly vigilant when pupils are undertaking their own search and will check that the children are following the agreed search plan;
* Pupils will be taught to use e-mail and the Internet responsibly in order to reduce the risk to themselves and others;
* The Online Safety Lead will monitor the effectiveness of Internet access by checking Futures Cloud weekly.
* The Headteacher will ensure that the policy is implemented effectively;

Generally, the above measures have been highly effective. However, due to the international scale and linked nature of information available via the Internet, it is not possible to guarantee that particular types of material will never appear on a computer screen. The school cannot accept liability for the material accessed, or any consequence of this.

A most important element of the Rules and Responsible Internet Use is that pupils will be taught to tell a teacher immediately if they encounter any material that makes them feel uncomfortable.

If there is an incident in which a pupil is exposed to offensive or upsetting material, responsibility for handling incidents involving children will be taken by the Headteacher and the pupil’s class teacher. All teaching staff will be made aware of the incident if appropriate.

Photographs

Prior permission is sought from all parents regarding the use of images for printed publications, media, website and videos. Staff should check the relevant year group permissions list before using images of children.

St. Giles’ & St. George’s C of E Academy Website: [www.stgilesstgeorgesacademy.co.uk](http://www.stgilesstgeorgesacademy.co.uk)

Our school website is intended to:

* Provide accurate, up-to-date information about our school.
* Enable pupils ‘achievements to be published for a wide audience including pupils, parents, staff, governors, members of the local community and others.
* Promote the school.

All classes can place items for publication on the school website. Class teachers will be responsible for ensuring that the content of the pupils’ work is accurate, the quality of presentation is maintained and that photo permission forms are checked before submitting the publication.

The point of contact on the school website will be the school address and telephone number. We do not publish pupil’s full names or identify individuals on our web pages. Home information or individual e-mail identities will not be published.

**Appendix 2: Acceptable use agreement (pupils and parents/carers)**

|  |  |
| --- | --- |
| **Acceptable use of the school’s ICT systems and internet: agreement for pupils and parents/carers** | |
| **Name of pupil:** | |
| **When using the school’s ICT systems and accessing the internet in school, I will not:**   * Use them for a non-educational purpose * Use them without a teacher being present, or without a teacher’s permission * Access any inappropriate websites * Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity) * Use chat rooms * 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 * Share my password with others or log in to the school’s network using someone else’s details * Give my personal information (including my name, address or telephone number) to anyone without the permission of my teacher or parent/carer * Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision   If I bring a personal mobile phone or other personal electronic device into school:   * 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.  I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others.  I will always use the school’s ICT systems and internet responsibly. | |
| **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 3: Acceptable use policy for staff and governors**

All members of staff have a responsibility to use the school’s computer system in a professional, lawful, and ethical manner. Our AUP must be fully complied with at all times. All users of the school network should note that it is monitored on a regular basis. Any person who is found to have misused the school system or not followed our AUP could face the following consequences:

* Temporary or permanent withdrawal from the school system
* Suspension or exclusion from the school
* Disciplinary action
* In the most serious cases legal action may also be taken.

Whilst our network and systems are organised to maintain the most secure environment possible **it is** **your responsibility to make sure the children you are directly working with are safe**. All adults working in school must do so under the guidance of the member of staff to whom they are responsible.

As an adult working in school you may be the first point of contact in dealing with incidents of ICT misuse or abuse. Every such incident must be reported to the Class Teacher who will then follow the procedures set out in our AUP.

Your key responsibilities are:

* Maintaining an appropriate level of professional conduct in your own internet use within school.
* Developing and maintaining knowledge of internet safety issues, particularly with regard to how they might affect children.
* Implementing our school AUP through effective classroom practice.
* Reporting any instances of ICT misuse to the Class Teacher who must report it to the E-Safety Coordinator in line with our school AUP. If the Class Teacher is suspected of being involved, report directly to the E-Safety Coordinator or Head Teacher.
* Supporting pupils who experience problems when using the internet, working with the Class Teacher.
* Using the internet and ICT facilities to ensure that internet safety is not compromised e.g. evaluating websites in advance of classroom use, using child oriented search engines.
* Embedding internet safety messages wherever possible.
* Following the school rules relating to acceptable use of our ICT equipment and other mobile technologies.
* Copies of our rules for pupil use of the network are displayed in the children’s planners. Please ensure you have read them and make sure the pupils you work with adhere to them.

**School ICT Network**

The school Network and associated services may be used for lawful purposes only.

**Passwords**

* Each child and adult working within the school must log on to the computers using the username and password given to them (class account or individual account). Passwords need to be kept a secret. Both adults and children need to fill in appropriate class computer/ipad logs, stating what time they logged onto the computer and what time they logged off. If for any reason a child or adult needs to leave their computer, they have to lock the computer to prevent others from using their account by pressing ‘Ctrl, Alt and Delete’.
* It is forbidden to use other children’s/adult’s/class accounts or files. Both adults and children will respect copyright and not copy anyone’s work and call it their own.

For the children in our school who are unable to understand the ‘Pupils Acceptable Usage Policy’ and for the children who are unable to log in and log off using their own password, the adult(s) working with those children will take full responsibility for their safe internet use in school.

**Software and Downloads**

* All users of the network must virus check any USB device storage devices before using on the network.

All users are prohibited from installing software onto the network from a CD-ROM, other device or by downloading from the Internet. If users need a new program installing onto the computer, our ICT Technician will be asked to do this if possible.

* Copyright and intellectual property rights must be respected when downloading from the internet.

**Personal Use**

The school recognises that occasional personal use of the school’s computer is beneficial both to the development of ICT skills and for maintaining a positive work-life balance. Such use is permitted, with the conditions that such use:

* Most comply with all other conditions of the AUP as they apply to non-personal use, and all other school policies regarding staff conduct.
* Must not interfere in any way with your other duties or those of any other member of staff.
* Must not have any undue effect on the performance of the computer system; and
* Must not be for any commercial purpose or gain unless explicitly authorised by the school.

Personal use is permitted at the discretion of the school and can be limited or revoked at any time.

**Email**

* All members of staff with a computer account in school are provided with a school email address for communication both internally and with other email users outside of school.
* No member of staff (including governors and non-teaching staff) must use non-school email accounts for any school/work related activity.
* Users are responsible for e-mail they send and should be aware that these are open to be read and should be treated as public.
* I am aware that email is not guaranteed to be private. Messages relating to or in support of illegal activities will be reported. Anonymous messages are not permitted.
* E-mail should be written carefully and politely and should never contain anything which is likely to cause annoyance, inconvenience or needless anxiety. Anonymous messages and chain letters must not be sent.
* When writing emails, you should use appropriate language. You should not use language that could be calculated to incite hatred against ethnic, religious or other minority. You need to remember that you are a representative of the school on a global public system. Illegal activities of any kind are strictly forbidden.
* E-mail attachments should only be opened if the source is known and trusted.
* Children are not permitted under any circumstances to e-mail a member of staff using their personal e-mail address. In addition, members of staff should not be emailing children using their personal email address.
* Privacy – I will not reveal any personal information (e.g. name, address, age, telephone number, social network details) of other users to any unauthorised person. I will not reveal any of my personal information to the pupils.
* I will not trespass into other users’ files or folders.
* I will ensure that all my login credentials (including passwords) are not shared with any other individuals, displayed or used by any individual than myself. Likewise, I will not share those of other users. I will ensure that if I think someone has learned my password then I will change it immediately and/or contact ICT technician.
* I will ensure that I log off after my session has finished. If I find an unattended machine logged on under another username I will not continue using the machine – I will log it off immediately.
* Any unsuitable communications received must be reported to a member of staff immediately.

**Images/Videos**

* All children need parental permission to have photographs or videos published electronically or in a public area even if they are unidentifiable.
* No photos or videos which include nudity or inappropriate actions are permitted to be taken or downloaded under any circumstance.

**Network Protocol**

* School computer and Internet use must be appropriate to a pupil's education or to staff professional activity.
* Respect other people’s material and do not corrupt, interfere with or destroy them.
* Do not open other people’s files without expressed permission.
* When working with personal data ensure that the data is secure.

**Internet Usage**

* Pupils must be supervised at all times when using the internet.
* Activities should be planned so ‘open searching is kept to a minimum. The facility for caching sites should be used prior to using the internet with pupils.
* When searching the internet with pupils, adults should encourage the children to use ‘child safe’ search engines. However safe search is set on all computers in school as a default on search engines.
* The use of social networking sites, public chat rooms and messaging systems (e.g. Facebook, Messenger, Twitter) is not allowed in school other than access to the school facebook page in the school office.
* Use the internet for personal financial gain, gambling, political purposes or advertising is forbidden.
* I will not attempt to visit websites that may be considered inappropriate or illegal. I am aware that downloading some material is illegal and that the police or other authorities may be called to investigate.

**Use of Social Networking Sites and Online Forums**

Staff must take care when using websites such as Facebook, Twitter, Dating Sites etc, even when such use occurs in their own time their own computer at home. Social Networking sites invite users to participate in informal ways that can leave you open to abuse, and often make little or no distinction between adult users and children.

You must not allow any pupil to access personal information you post on a social networking site. In particular:

* You must not add a pupil to your ‘friends list’, nor invite them to be friends with you.
* You must ensure that personal information is not accessible via ‘Public’ setting, but ensure it is to a ‘Friends only’ level of visibility.
* You should avoid contacting any pupil privately via social networking site, even for school-related purposes.
* You should take steps to ensure that any person contacting you via a social networking website is who they claim to be, and not an imposter, before allowing them to access to your personal information.

It is advised not to accept invitations from the pupils’ parents or careers to add me as a friend to their social networking sites, nor should you invite them to be your friends. As damage to professional reputations can inadvertently be caused by quite innocent postings or images. You will need to ensure that any private social networking sites/blogs that you create or actively contribute to are not to be confused with your professional role in anyway.

Staff should also take care when posting to any public website (including online discussion forums or blogs) that their comments do not harm their professional standing or the reputation of the school – even if their online activities are entirely unrelated to the school.

* Unless authorised to do so, you must not post comments on websites that may appear as if you are speaking for the school.
* You should not post any material online that can be clearly linked to the school that may damage the school’s reputation.
* You should avoid posting any material clearly identifying yourself, another member of staff, or a pupil, that could potentially be used to embarrass, harass or defame the subject.

**Use of your own Equipment**

* Any mains-operated personal computer or electrical equipment brought on site, for any use, is subject to a Portable Appliance Test (PAT) by site maintenance staff, and must not be used until approved. This test must be performed at regular intervals as required by school’s normal rules on electrical safety testing.
* You must not connect personal computer equipment to school computer equipment without prior approval from ICT Technician, without the exception of storage devices such as USB memory sticks.

**Mobile Devices**

* Personal mobile phones should not be used in areas of school where pupils have access.
* During teaching time, mobile phones should be turned off or put on silent mode and stored in a cupboard away from the children.
* Adult are allowed to access their personal phones on breaks, lunch times and after school in designated areas e.g. staff room or teachers room (safe, suitable places where the children are not present).
* It is forbidden to take photographs/videos of the children on personal mobile phones.
* No images of the children should be taken without parental consent and permission from a member of staff using any mobile device e.g. phones, school cameras. These devices must not be removed from the school premises if they contain images of pupils and without permission from a member of staff.

**Supervision of Pupil Use**

* Pupils must be supervised at all times when using school computer equipment. Supervising staff needs to ensure that pupils have signed the class computer/ipad log and if the pupils are unable to sign the log book they are responsible for doing it for them. When arranging use of computer facilities for pupils, you must ensure supervision is available.
* Supervising staff are responsible for ensuring that the separate Acceptable Use Policy for pupils is enforced.
* Supervising staff must ensure they have read and understand the separate guidelines on e-safety, which pertains to the child protection issues of computer use by pupils.

**Reporting Problems with the Computer System**

It is the job of the ICT Technician to ensure that the school computer system is working optimally at all times and that any faults are rectified as soon as possible.

* You should report any problems that need attention to ICT Technician.
* If you suspect your computer has been affected by a virus or other malware, you must report this to ICT Technician immediately.
* If you have lost documents or files, you should report this as soon as possible. The longer a data loss problem goes unreported, the less chances of your data being recoverable.

**Reporting Breaches of this Policy**

All members of staff have a duty to ensure this Acceptable Use Policy is followed. You must immediately inform the Head Teacher, of abuse of any part of the computer system. In particular, you should report:

* Any websites accessible from within school that you feel are unsuitable for staff or pupil consumption.
* Any inappropriate content suspected to be stored on the computer system. This may be contained in email, documents, pictures, etc.
* Any breaches, or attempted breaches, of computer security, or
* Any instance of bullying or harassment suffered by you, another member of staff, or a pupil via the school computer system.

All reports will be treated confidentially.

**Electronic Devices - Searching & Deletion**

In accordance to ‘The Education Act 2012’ school has the right to search and or delete anything from personal devices if they believe illegal or suspicious activity is taken place.

**Exemptions**

All the above stands unless given permission from the Head Teacher e.g. while on residential trips, permission may be given to designated staff to upload photos for St. Giles’ & St. George’s Facebook account.

All staff, governors, volunteers and visitors who will be using the online systems in school must read and sign Appendix 4.

# Appendix 4: acceptable use agreement (staff, governors, volunteers and visitors)

|  |  |
| --- | --- |
| **Acceptable use of the school’s ICT systems and the internet: agreement for 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, I will not:   * Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature * 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 * Share my password with others or log in to the school’s network using someone else’s details | |
| 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.  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:** |

# Appendix 5: online safety training needs – self-audit for staff

|  |  |  |
| --- | --- | --- |
| **Online safety training needs audit** | | |
| **Name of staff member/volunteer:** | | **Date:** |
| Do you know the name of the person who has lead responsibility for online safety in school? | |  |
| Do you know what you must do if a pupil approaches you with a concern or issue? | |  |
| Are you familiar with the school’s acceptable use agreement for staff, volunteers, governors and visitors? | |  |
| Are you familiar with the school’s acceptable use agreement for pupils and parents? | |  |
| Do you regularly change your password for accessing the school’s ICT systems? | |  |
| Are you familiar with the school’s approach to tackling cyber-bullying? | |  |
| Are there any areas of online safety in which you would like training/further training? Please record them here. |  | |

**Appendix 6: Futures Cloud Incidents Log**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date and Time** | **Incident** | **RAG** | **Action** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |