STROUD SCHOOL: E-SAFETY & MOBILE DEVICE POLICY

This policy is applicable to all pupils including those in the EYFS

The School recognises that ICT and the internet are fantastic tools for learning and communication that can be used in School to enhance the curriculum, challenge pupils, and support creativity and independence. Using ICT to interact socially and share ideas can benefit everyone in the School community, but it is important that the use of the internet and ICT is seen as a responsibility and that pupils, staff and parents use it appropriately and practice good e-safety. It is important that all members of the School community are aware of the dangers of using the internet and how they should conduct themselves online.

E-safety covers the internet but it also covers mobile phones/devices, iPads and other electronic communications technologies. We know that some adults and young people will use these technologies to harm children. There is a 'duty of care' for any persons working with children and educating all members of the School community on the risks and responsibilities of e-safety falls under this duty. It is important that there is a balance between controlling access to the internet and technology and allowing freedom to explore and use these tools to their full potential. This policy aims to be an aid in regulating ICT activity in School, and provide a good understanding of appropriate ICT use that members of the School community can use as a reference for their conduct online outside of school hours. E-safety is a whole-school issue and responsibility.

Cyber-bullying by pupils will be treated as seriously as any other type of bullying and will be managed through our anti-bullying policy and procedures.

1. Roles and responsibility

The Head and Governors will ensure that the E-safety policy is implemented and compliance with the policy monitored but the day-to-day management of E-safety in the School is the responsibility of the Head of IT. They will work closely with the Deputy Head, Heads of Department and PSHEE Curriculum Team in this regard.

The Head of IT is trained to alert the DSL to any concern about accessing content or cyber-bullying. It then might be necessary to contact children's social care services if a child is likely to be harmed.

2. Communicating School policy

All staff are provided with a copy of the E-safety policy and this policy is available on the open 'Policies' section of the School website for parents, staff, and pupils to access when and as they wish. Rules relating to the School Code of Conduct when online, and E-safety guidelines, are displayed around the School. E-safety is integrated into the curriculum in any circumstance where the internet or technology are being used, as well as being specifically addressed in the ICT and PSHeE curriculum.

On joining the School, parents will be made aware of the ICT Code of Conduct and AUP relevant to the age of their child. When children move into the Middle School, or join the school after Y3, they will be required to sign a Code of Conduct which parents will be required to counter sign.

Staff are provided with a Staff Code of Conduct and AUP which they are expected to sign and adhere to.

3. Making use of ICT and the internet in School

Using ICT and the internet in School brings many benefits to pupils, staff and parents. The internet is used in School to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the School's management functions. Technology is advancing rapidly and is now a huge part of everyday life, education and business. We want to equip our pupils with all the necessary ICT skills that they will need in order

to enable them to progress confidently into the next stage of their education, and professional working environment when they leave school.

In common with other media such as magazines, books and video, some material available via the internet is unsuitable for pupils. 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 or child's mobile device. The School cannot accept liability for the material accessed, or any consequences of internet access.

Expectations of use of School computers apply to staff and pupils both in and out of lessons.

4. Learning to evaluate internet content

With so much information available online it is important that pupils learn how to evaluate internet content for accuracy and intent. This is approached by the School as part of digital literacy across all subjects in the curriculum. Pupils will be taught:

- to be critically aware of materials they read, and shown how to validate information before accepting it as accurate;
- to respect copyright.

If staff or pupils discover unsuitable sites then the URL, time, date and content must be reported to the IT Department. Any material found by members of the School community that is believed to be unlawful will be reported to the appropriate agencies via the IT Department or a member of the Senior Management Team. Regular checks will take place to ensure that filtering services are working effectively.

5. Managing information systems

The School is responsible for reviewing and managing the security of the computers and internet networks as a whole and takes the protection of School data and personal protection of our School community very seriously. This means protecting the School network, as far as is practicably possible, against viruses, hackers and other external security threats. The security of the School information systems and users will be reviewed regularly by the IT Support team, led by the Network Manager and virus protection software will be updated regularly. Some safeguards that the School takes to secure our computer systems are:

- Making sure that unapproved software is not downloaded to any School computers. Files held on the School network will be regularly checked for viruses;
- The use of user logins and passwords to access the School network will be enforced;
- Portable media containing School data or programmes must be password protected and devices will be monitored periodically be the Head of IT.

For more information on data protection in School please refer to our Privacy Notice which can be accessed on the School's website. More information on protecting personal data can be found in section 11 of this policy.

6. Emails

The School uses email internally for staff and pupils, and externally for contacting parents, and is an essential part of school communication.

Access in School to external personal email accounts may be blocked. The School has the right to monitor emails and their contents but will only do so if there is suspicion of inappropriate use.

6.1 School email accounts and appropriate use

Staff should be aware of the following when using email in School:

- Staff should only use official School email accounts for school-related matters, contact with other professionals for work purposes and to communicate with pupils, parents or carers. Personal email accounts should not be used to contact any of these people.
- Emails sent from School accounts should be professionally and carefully written. Staff are representing the School at all times and should take this into account when entering into any email communications.
- For any awkward, sensitive, easily misinterpreted situations or anything that may have legal repercussions, staff should have the content of their email checked carefully by the Head or Deputy.
- Staff must tell a member of the Senior Management Team if they receive any offensive, threatening or unsuitable emails either from within the School or from an external account. They should not attempt to deal with this themselves.
- The forwarding of chain messages is not permitted in School.
- Further advice regarding email communication for staff is provided in the Correspondence section of the Staff Handbook and the guidance on email etiquette.

Pupils should be aware of the following when using email in School, and will be taught to follow these guidelines through the ICT curriculum and in any instance where email is being used within the curriculum or in class:

- All pupils are provided with a School email account and pupils may only use approved email accounts on the School system.
- Pupils are warned not to reveal personal details of themselves or others in email communication, or arrange to meet anyone. Social emailing can interfere with learning and will be restricted.
- Pupils should immediately inform a member of staff if they receive any offensive, threatening or unsuitable emails either from within the School or from an external account. They should not attempt to deal with this themselves.

7. Published content and the School website

The School website is viewed as a useful tool for communicating our School ethos and practice to the wider community. It is also a valuable resource for parents, pupils and staff for keeping up-to-date with School news and events, celebrating whole-school achievements, personal achievements and promoting School projects.
The website is in the public domain, and can be viewed by anybody online. Any information published on the website will be carefully considered in terms of safety for the School community, copyrights and privacy policies. No personal information on staff or pupils will be published. For information on the School policy on children's photographs on the School website please refer to section 7.1 of this policy.

The Deputy Head is responsible for publishing and maintaining the content of the School website. The website will comply with the School's guidelines for publications including respect for intellectual property rights and copyright. Staff and pupils will be made aware of copyright in respect of material taken from the internet.

Pupils should not publish anything on the internet involving the School unless permission has been granted by the Head or Deputy Head.

7.1 Policy and guidance of safe use of children's photographs and work

Colour photographs and pupils work bring our School to life, showcase our pupils' talents, and add interest to publications both online and in print that represent the School. However, the School acknowledges the importance of having safety precautions in place to prevent the misuse of such material.

Under GDPR guidance images of pupils and staff will not be displayed in public, either in print or online, without consent (as per parental consent form within the Parent Portal).

In conjunction with a child's health care plan a picture is displayed on the staffroom notice board, along with the child's full name, to identify those pupils who have any severe medical conditions that staff need to be aware of.

Using photographs of individual children

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying, and safeguarding concerns to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

It is important that published images do not identify pupils or put them at risk of being identified. Only images created by or for the School will be used in public and children may not be approached or photographed while in School or doing School activities without the School's permission, with the exception of parents taking photographs or videos at School events involving their son or daughter for personal use only (as defined by the Information Commissioner's Office ICO).
The School follows general rules on the use of photographs of individual children:

- Consent from parents will cover the use of images in:
    - all School publications
    - on the School website
    - in videos made by the School or in class for School projects.
- Unpublished electronic and paper images will be stored securely.
- Images will be carefully chosen to ensure that they do not pose a risk of misuse. This includes ensuring that pupils are appropriately dressed. Photographs of activities which may pose a greater risk of potential misuse (for example, swimming activities), will focus more on the sport than the pupils (i.e. a pupil in a swimming pool, rather than standing by the side in a swimsuit).
- For public documents, including in newspapers, full names will not be published alongside images of the child without the written permission from parents. Groups may be referred to collectively by year group or form name.
- Events recorded by family members of the pupils such as School drama productions or sports events must be used for personal use only and a senior member of staff will remind all attendees of this at school events.
- Pupils are encouraged to tell a member of staff if they are concerned or uncomfortable with any photographs that are taken of them or they are being asked to participate in.
- Any photographers that are commissioned by the School will be fully briefed on appropriateness in terms of content and behaviour, will wear identification at all times, and will not have unsupervised access to the pupils.

7.2 Complaints of misuse of photographs or video

Parents should follow standard School complaints procedure if they have a concern or complaint regarding the misuse of School photographs. Please refer to our complaints policy for more information on the steps to take when making a complaint. Any issues or sanctions will be dealt with in line with School policy.

7.3 Social networking, social media and personal publishing

Personal publishing tools include blogs, wikis, social networking sites, bulletin boards, chat rooms and instant messaging programmes. These online forums are the more obvious sources of inappropriate and harmful behaviour and where pupils are most vulnerable to being contacted by a dangerous person. It is important that we educate pupils so that they can make their own informed decisions and take responsibility for their conduct online. The School will normally block/filter access to social networking sites via the School network.

Social media sites have many benefits, however both staff and pupils should be aware of how they present themselves online. Pupils are taught through the ICT curriculum and PSHE about the risks and responsibility of uploading personal information and the difficulty of taking it down completely once it is out in such a public place.

The School follows general rules on the use of social media and social networking sites in School:

- Pupils are educated on the dangers of social networking sites and how to use them in safe and productive ways. Pupils are advised never to give out personal details of any kind which may identify them or their location. They are all made fully aware of the School's code of conduct regarding the use of ICT and technologies and behaviour online.
- Any sites that are to be used in class will be risk-assessed by the teacher in charge prior to the lesson to ensure that the site is age-appropriate and safe for use.
- Official School blogs created by staff or pupils/year groups/School clubs as part of the School curriculum will be moderated by a member of staff.
- Pupils and staff are encouraged not to publish specific and detailed private thoughts, especially those that might be considered hurtful, harmful or defamatory. The School expects all staff and pupils to remember that they are representing the School at all times and must act appropriately on social media and in public when online.
- Safe and professional behaviour of staff online will be discussed at staff induction and guidance is provided through the ICT Staff code of conduct and AUP.

8. Mobile phones and personal devices

Mobile phones and other personal devices are now an important part of everyone's life and have considerable value, particularly in relation to individual safety. Whilst these devices are commonplace in today's society, their use and the responsibility for using them should not be taken lightly. Some issues surrounding the possession of these devices are that:

- they can make pupils and staff more vulnerable to cyberbullying;
- they can be used to access inappropriate internet material;
- they can be a distraction in the classroom;
- they are valuable items that could be stolen, damaged, or lost;
- they can have integrated cameras, which can lead to child protection, bullying and data protection issues.

The School's expectation is that mobile devices, where permitted, will be used responsibly at all times and certain measures are taken to ensure that pupils adhere to this expectation. Some of these are outlined below. Pupils must only use these devices in lessons under the direction of the teacher, unless permission has been sought from the teacher.

- Pupils are not permitted to bring mobile phones to school except where express permission has been granted by the Head or Deputy Head.
- Where a pupil has been given permission to bring a mobile phone to school, it must be stored safely by a member of staff during the day.
- The School will not tolerate cyberbullying against either pupils or staff. Sending inappropriate, suggestive or abusive messages is forbidden and anyone who is found to have sent a message of such content will be disciplined. For more information on the School's disciplinary sanctions read the School's Behaviour, Rewards and Sanctions policy.
- In the Senior School, where pupils are permitted to have 1:1 devices, iPads can be confiscated by a member of staff, and the device can be searched by nominated senior members of staff if there is reason to believe that there may be evidence of harmful or inappropriate use on the device.
- Individual pupils are responsible for their own mobile devices and should ensure that they take care of them at all times. The normal disciplinary procedures apply in the event of damage to another pupil's property.
- Headphones must not be worn during lessons unless permission is given by the teacher.
- Pupils must not use these devices to broadcast music unless permission to do so has been given. Pupils must ensure that files stored do not contain violent or pornographic images or other material that is likely to cause offence. In very serious cases the police may be contacted.
- The use of mobile phones by pupils on School trips is at the discretion of the trip leader.
- Social media and messaging are not to be accessed during class time unless as part of a directed teaching activity.

- Video, audio and photographic recording must not take place without the consent of student(s) and teacher(s). Consent must be explicit, not implied.

It should be noted that power supplies for these devices must not be brought to School as all electrical devices used in the School must be PAT tested.

8.1 Mobile phone or personal device misuse

Pupils

- Pupils who breach School policy relating to the use of personal devices will be disciplined in line with the School's Behaviour, Rewards and Sanctions policy. Their mobile phone may be confiscated if brought onto the school site. In the event of confiscation the member of staff will make arrangements for its return, which would normally be at the end of the School day.
- Pupils are under no circumstances allowed to bring personal devices into examination rooms with them.
- Pupils are not permitted, in any circumstances, to use their phones or mobile devices in the toilet area or where children are changing or being changed.

Teaching and Non-Teaching Staff

- Staff are strongly advised not to use their own personal devices to contact pupils or parents either in or out of School time.
- Staff should use School equipment if photos or videos are being taken as part of the curriculum or in a professional capacity. Where a personal device is used images and videos should be downloaded to the network and not stored for longer than necessary.
- Calls or texts should not be taken or made during lesson time or during any other contact time with children. Where express permission has been granted by the Head or Deputy Head, phones may be kept on at a low volume.
- Staff are not permitted, in any circumstances, to use their phones or mobile devices in the toilet area or where children are changing or being changed.
- Staff should not, under any circumstances, use their personal phones, cameras or mobile devices to take images or make recordings of children in the Early Years building.
- The School expects staff to lead by example. Personal mobile phones should be switched off or on silent during School hours and personal use limited to staff breaks or outside of the school day.
- Any breach of School policy may result in disciplinary action against that member of staff.

Parents and Visitors

- Calls or texts should not be taken or made around children who are in session.
- Parents and visitors are not permitted, under any circumstances, to use their phones or mobile devices, or take images or make recordings of children on a camera, mobile phone or other mobile device in the Early Years building.

9. Cyberbullying

Cyberbullying including peer on peer abuse, as with any other form of bullying, is taken very seriously by the School. Information about specific strategies to prevent and tackle bullying are set out in the School's Anti-bullying policy. The anonymity that can come with using the internet can sometimes make people feel safe to say and do hurtful things that they otherwise would not do in person. It is made very clear to members of the School community what is expected of them in terms of respecting their peers, members of the public and staff, and any intentional breach of this will result in disciplinary action.

If an allegation of bullying does come up, the School will:

- take it seriously;
- act as quickly as possible to establish the facts. It may be necessary to examine School systems and logs or contact the service provider in order to identify the bully;

- record and report the incident;
- provide support and reassurance to the victim;
- make it clear to the 'bully' that this behaviour will not be tolerated. If there is a group of people involved, they will be spoken to individually and as a whole group. It is important that children who have harmed another, either physically or emotionally, redress their actions and the School will make sure that they understand what they have done and the impact of their actions.

If a sanction is used, it will correlate to the seriousness of the incident and the 'bully' will be told why it is being used. They will be asked to remove any harmful or inappropriate content that has been published, and the service provider may be contacted to do this if they refuse or are unable to remove it. They may have their internet access suspended in School.

All staff and pupils are trained in online safety every other year including aspects such as peer on peer abuse and PREVENT. Online Safety and mobile device seminars are run annually for parents. Pupils receive e-safety training as part of their ongoing ICT and PSHEE lessons.

More information can be accessed from non-statutory Department of Education advice: Cyberbullying: Advice for headteachers and school staff (2014) and Advice for parents and carers on cyberbullying (2014).

10. Managing emerging technologies

Technology is progressing rapidly and new technologies are emerging all the time. The School will risk-assess any new technologies before they are allowed in School, and will consider any educational benefits that they might have. The School keeps up-to-date with new technologies and is prepared to quickly develop appropriate strategies for dealing with new technological developments.

11. Protecting personal data

The School believes that protecting the privacy of our staff and pupils and regulating their safety through data management, control and evaluation is vital to whole-school and individual progress. The School collects personal data from pupils, parents, and staff and processes it in order to support teaching and learning, monitor and report on pupil and teacher progress, and strengthen our pastoral provision.

We take responsibility for ensuring that any data that we collect and process is used correctly and only as is necessary, and the School will keep parents fully informed of the how data is collected, what is collected, and how it is used. Results, attendance and registration records, special educational needs data, and any relevant medical information are examples of the type of data that the School needs. Through effective data management we can monitor a range of School provisions and evaluate the well-being and academic progression of our School body to ensure that we are doing all we can to support both staff and students.

In line with the Data Protection Act (2018), and following principles of good practice when processing data, the School will ensure that all personal data is:

- Used fairly, lawfully and transparently;
- Used for specified, explicit purposes;
- Used in a way that is adequate, relevant and limited to only what is necessary;
- Accurate and where necessary, kept up-to-date;
- Kept for no longer than is necessary;
- Handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage.

There may be circumstances where the School is required either by law or in the best interests of our students or staff to pass information onto external authorities; for example, our local authority or the Department of Health.

These authorities are up-to-date with data protection law and have their own policies relating to the protection of any data that they receive or collect.

For more information on the School's safeguarding relating to data protection, please request a copy of the School's data protection policy.

Related Documents
ICT Code of Conduct and Acceptable Use Policy (AUP) – Staff
ICT Code of Conduct and Acceptable Use Policy (AUP) – EY and KS1
ICT Code of Conduct and Acceptable Use Policy (AUP) – Middle and Senior School
Data Protection Policy
Anti-bullying Policy
Parent Contract
Safeguarding Policy
PSHEE Policy

Appendix 1:

Middle School and Senior School ICT Code of Conduct and AUP

Stroud School: ICT Code of Conduct and Acceptable Use Policy (AUP)

Your agreement to follow these guidelines ensures your safety and the efficient functioning of the School's ICT facilities:

Definition

The ICT facilities at Stroud are defined as computers, iPads, software, monitors, keyboards, mice, printers, scanners, cameras, camcorders and any other electronic item. The ICT facilities at Stroud also include: telephones, mobile phones, fax machines, televisions and DVD players and any other electrical device. Internet, E-mail and the network are also included as ICT facilities.

Copyright

You must not copy work from other people or copy and paste from online sources without reference to the original author. If you use the internet for research you must put the research into your own words.

Software

You may not install software on any school computer.

Passwords

Keep your password safe, treat it like your toothbrush and never share it.

Storage Areas

You are responsible for keeping your user area, the area where you save your work, tidy. School can look at your files to make sure you are using the system sensibly.

Printing

You should only print work when necessary and with the permission of your teacher.

The Internet

The Internet is there for you to use for research and school work. When you use it you must be sensible. Your teachers will show you how. Everything you do on the computer is monitored and the ICT Department is authorised to check that you are using email and the internet in a sensible and responsible way.

Personal Details

You should keep personal details safe at all times, including your full name, address, telephone number, passwords, parents details and details of events that you, family or friends are attending.

Images

You should not send images of yourself, or any other members of the school community, outside of school without a teacher's permission. You should never take mobile devises with cameras into the toilets or any area where children are changing.

Time wasting

The ICT facilities at school are to be used for school work. On-line games will only be allowed with the permission of the teacher or responsible adult. Some on-line games will be blocked.

Email and messaging

You will be given a school email address to send or receive work. This will allow access to Gsuite applications, be a line of communication with your teacher and allow for the setting of prep. Use of any external email, messaging and online chat software is not allowed at school.

Privacy

If you wish for your Child's email account to be restricted to internal use only please email it@stroud-kes.org.uk

Social Networking Websites

Many Social Networking sites have an age restriction which you should know, and adhere to. The use of Social Networking websites (e.g. Facebook) is not allowed in school. When using Social Networking sites at home, you must not use any insulting or offensive material of any kind about any other member of the school community, or the school itself. This may be dealt with as part of the school normal behaviour policies.

External Proxy Websites and Anonymizers

If a website is blocked, it is for important reasons. You must not under any circumstances continue to try to access the site by using an External Proxy or Anonymizer Site. External Proxies and Anonymizers are websites which attempt to hide the user details, and by doing this, bypass the filtering system.

Mobile Phones

Mobile phones are not allowed at Stroud without the express permission of the Head. This includes 4G enabled watches and devices.

Unacceptable use of ICT

The following will be dealt with in the same way as any other form of unacceptable behaviour in school:
Sending or displaying offensive messages or pictures;
Using bad language, insulting or being unkind to others;
Using the internet to frighten or annoy another person;
Damaging computers, computer systems or networks;
Sending rude messages from mobile phones or any other device;
Using other pupils' passwords and trespassing in other people's folders.

This list is not exhaustive and behaviour that is deemed inappropriate will be dealt with on a case by case basis in accordance with school policies.

Sanctions

If you break any of these rules you may be banned from using ICT at School. This may be a temporary or permanent ban depending on the seriousness of the offence. All pupils will be subject to sanctions as per our behaviour policies.

Stroud ICT Acceptable Use Policy Reply Slip

Pupil's Name: ……. Form: ……

As a user of the School ICT facilities, I agree to comply with the school rules governing their use as set out above.

Signed (Pupil): ……. Date: ……..

Parent/ Guardian

As the parent or legal guardian of the pupil signing the above, I give permission for them to use the Internet and e-mail. I understand my child will be held accountable for their actions. I accept responsibility for setting standards for them to follow when selecting, sharing and exploring information and media.

Signed: …… Print name: ……

Date: ……

Please return to the Registrar together with all acceptance paperwork prior to your child starting at Stroud.

Thank you.

Appendix 2:

EY and KS1 ICT Code of Conduct and AUP

Stroud School: Early Years and KS1 ICT Code of Conduct

Rationale
The ICT facilities at Stroud are defined as computers, iPads, software, monitors, keyboards, mice, printers, scanners, cameras, camcorders and any other electronic item. The ICT facilities at Stroud also include: telephones, mobile phones, fax machines, televisions and DVD players and any other electrical device. Internet, E-mail and the network are also included as ICT facilities.

Children in the early Years and KS1 are given the opportunities to become literate with the use of ICT including the internet and mobile devices such as iPads. The use of technology pervades all areas of the EYFS and KS1 curriculum. Therefore we need to ensure children develop a confidence in using ICT and an understanding of responsible use of technology from an early age.

Parents are required to help their children to follow these guidelines to ensure their safety and the efficient functioning of the School's ICT facilities. This document should be read in conjunction with the E-Safety & Mobile Devices Policy for further information on internet filtering, use of images.

Passwords
Password are a way to keep your information safe – a bit like a key to your computer. Try to learn your log-in details. In Year 2 you will get a password - you must keep your password safe, treat it like your toothbrush and never share it.

Printing
You should only print work when your teacher has said you can.

The Internet
The Internet can help us find all sorts of interesting information. When you use it you must be sensible. Your teachers will show you how.

All about me
You should never tell anybody about yourself on the computer, unless it is for a piece of work in school. This is the same as being safe and not talking to strangers.

Pictures of me and my friends
In school you or your teacher might take photos to put on the wall or to stick in your books. Sometimes mummies and daddies will take photos of school plays and sports days. No one else should take photos of you and you should tell a teacher if you are worried.

Mobile Phones
Children are not allowed to bring mobile phones to school. If you see someone with a mobile phone you should tell your teacher.

Using the computers
We should never:
Send messages or pictures that will make people sad
Say mean things or be unkind to others
Try to break the computers on purpose

Stroud School: Early Years and KS1 ICT Code of Conduct

As the parent or legal guardian of the pupil named below, I understand that the Internet will be used at school. I will support my child in using computers responsibly and I accept responsibility for setting standards for them to follow.

Name of child: …… Form: ……

Signed: …… Print name: ……

Date: ……

Please return to the Registrar together with all acceptance paperwork prior to your child starting at Stroud.

Thank you.

Appendix 3:

Staff ICT Code of Conduct and AUP

Stroud School: Staff ICT Code of Conduct and Acceptable Use Policy (AUP)

This policy is applicable to all staff including those working in the EYFS

This policy should be read in conjunction with the E-Safety policy.

This document sets out the schools policy with regard to the use of the internet and the use of school equipment and applications by all non-pupil users of the school network, including teaching and non-teaching staff, children and partners of staff, and visitors.

ICT includes a wide range of systems, including mobile phones, mobile devices, digital cameras, email, social networking and may also include personal ICT devices when used for school business or machines connected to the internet through the school network.

In the course of their work, some staff may have access to confidential information, including files, emails and activity patterns of other staff. It is considered a serious breach of the terms and conditions of employment for such staff to deliberately access confidential information without due cause. Confidential information seen must only be used for legitimate work related matters and must not be disclosed to third parties. Any breach of confidence of this nature will be treated as a serious disciplinary offence and may in some cases be regarded as gross misconduct.

Security and data use:

- Great care must be taken to ensure personal access passwords remain confidential to avoid misuse by others. Staff passwords permit access to privileged, confidential data. Staff must not disclose any password or security information to anyone other than an authorised system manager.
- Personal data must be stored securely and used appropriately in accordance with the Data Protection Policy, whether in school, taken off the school premises or accessed remotely. Sensitive data should not be stored outside the school systems.
- Personal details of any colleague or pupil must not be released (over the internet or otherwise) including phone numbers, fax numbers or personal addresses and home email accounts.
- Other people's files should not be opened or modified without their permission.
- Copyright and intellectual property rights must be adhered to, including acknowledgement of sources used.

Appropriate use:

- Staff should not attempt to visit sites containing dubious or immoral material which might be considered inappropriate – in other words, material which a reasonable individual would consider to be inappropriate, including, but not limited to, pornographic, racist, sexist, or violent material.
- Use of school Internet access for business, profit, advertising, or political purposes is strictly forbidden.
- Deliberate access of inappropriate material by employees would be regarded by the School as a significant breach of trust, or, for certain materials or sites, gross misconduct, which may result in the School taking disciplinary action. It should also be noted that downloading some material is illegal and the police or other authorities may be called to investigate.
- Clearly, access to other inappropriate or offensive sites should be avoided. However, there may be circumstances where access to such material is necessary to inform teaching and learning. In such cases, prior written permission to use such material should be obtained from the Head.

Accidental access:

If inappropriate material is inadvertently accessed or received by pupils or staff, this must be reported immediately to the Head of IT, the Child Protection Liaison Officer (the Deputy Head) and the network manager.

Monitoring:

Internet users leave a record of everything they have looked at and of all emails sent or received. Website access at School if filtered, in order to fulfil our duty of care. The school may exercise its right to monitor the use of the School's information systems and Internet access, to intercept e-mail and to delete inappropriate materials where it believes unauthorised use of the school's information systems may be taking place, or the system may be being used for criminal purposes or storing unauthorised or unlawful text, imagery or sound.

Contacting pupils:

Electronic communications with pupils including email, instant messaging (IM) and social networking is not permitted unless through the monitored and safe use of the School's Virtual Learning Environment (VLE). Staff should be aware of the professional risks involved in communicating with pupils via instant messaging, mobile phone or text messaging and care should be taken to ensure that messages in any form cannot be misunderstood or misinterpreted. Staff should not respond to invitations from current pupils or past pupils who are still in full time education via any social networking sites. If it is necessary to contact pupils electronically staff should use the VLE, School email system, iSAMS or Firefly Planner. The school system provides an "audit trail", for protection, which is not necessarily present in other systems.

Contacting parents:

Staff should also be aware of the professional risks involved in communicating with parents via instant messaging, mobile phone or text messaging and care should be taken to ensure that messages in any form cannot be misunderstood or misinterpreted.

Staff should be aware of the risk of reputational damage, and potential defamation, which can be caused by inappropriate contact and comments with parents outside of a professional setting. Boundaries can be blurred when staff are also parents and as such, they need to be aware that they are always representing the school.

If it is necessary to contact parents electronically staff should use the School email system and involve the ensure emails are checked by the Head or Deputy Head if going to groups of parents. The school system provides an "audit trail", for protection, which is not necessarily present in other systems.

Contribution to other websites:

Where staff author for or contribute to other websites (including blogs, forums or wikis or social networking) they should ensure that the site does not judge or defame the school, colleagues or the school community, and does not identify pupils either by name or in photographs.

Downloading software:

Downloading software and other data from the internet onto the school network or storage device should be undertaken with caution in order to protect against viruses and also to ensure copyright compliance. Software should only be installed on School equipment by the ICT department. If in doubt, advice should be sought from the Head of IT or the Network manager.

Personal use of facilities:

Facilities are made available by the School and are provided for work related activities. This applies equally to School internet and e-mail facilities, whether within the School building or outside it. Staff are permitted to make personal use of e-mail and internet facilities provided that this does not interfere with the performance of their duties.

Laptop and iPad use:

Laptops and iPads provide the convenience of portability. This convenience exposes the school and the device to certain risks. These include but are not limited to: theft of school property; exposure of sensitive data or information; damage of school property.

All members of staff must take appropriate care to protect their laptop or iPad from theft or damage. Electronic devices should not:

- be left out overnight in classrooms
- be left unattended in a parked car (where unavoidable, the device should be in a locked boot out of sight).
- be used in environments where they may come to harm i.e. in extremes of temperature, humidity or in outdoor environments without appropriate protection.
- be lent to or used by others
- be stored inappropriately e.g. under heavy objects

Electronic devices should be:

- placed out of easy line of vision (i.e. in a cupboard or drawer)
- carried and stored in an appropriate case with padded protection, or corner guards for iPads
- have robust passwords and log-in details that are not shared with anyone
- logged off, or locked, when unattended.

In line with the E-Safety and Mobile Devices Policy – staff should only take photos for school purposes and in line with any photo permission restrictions. Images of children should be downloaded to the school network and not stored on mobile devices or laptops for longer than necessary.

Laptops and iPads remain the property of the School at all times. Any damage or loss must be reported to the Head of IT. The School will not be responsible for the financial or other loss resulting from personal files deleted from an iPad or laptop.

Staff Name _____

As a user of the School ICT facilities, I agree to comply with the school rules governing their use as set out above and in the E-Safety and Mobile Devices Policy which I have read and understood. I am aware that in the event that this policy is breached I may be subject to sanctions which could include, but are not limited to: disciplinary procedures; temporary or permanent restrictions of network access; or, temporary or permanent revocation of network rights.

Signed _____ **Date** _____