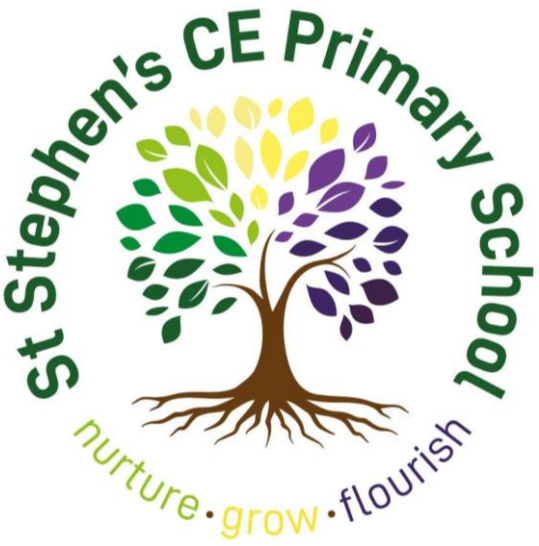

ICT Acceptable Use Policy

Contents:

	Statement of intent	2
1.	Introduction	3
2.	General code of practice	4
3.	Internet code of practice	7
4.	Email code of practice	10
5.	Emails - advice to staff	13
6.	Social Media Code of Practice	13
7.	Mobile Devices	17
8.	Working from home	17
9.	Training	18
10.	Reporting misuse	18
11.	Signing this ICT Acceptable Use Policy	19
12.	Annex 1 - Pupil ICT Acceptable Use	20

Statement of intent

Whilst our school promotes the use of technology and understands the positive effects it can have on enhancing pupils' learning and community engagement, we must also ensure that technology is used appropriately. Any misuse of technology will not be taken lightly and will be reported to the Headteacher in order for any necessary further action to be taken.

This Acceptable Use Policy is designed to outline staff responsibilities when using technology, whether this is via personal devices or school devices, or on/off the school premises, and applies to all staff, volunteers, contractors and visitors.

Our school provides laptops and digital equipment to some staff to assist in the planning and delivery of the curriculum. The laptop and any accessories provided with it remains the property of St Stephen's school and is for your sole use.

Introduction

1.1. This policy applies to all employees, volunteers, supply staff and contractors using school ICT facilities.
1.2. This policy should be read in conjunction with the school's Data Protection Policy, and Records Management Policy.
1.3. This policy is non contractual and may be amended at any time. Breach of this policy may potentially give rise to disciplinary action.

General code of practice

1.4. The school has well-developed and advanced ICT systems, which it intends you to benefit from.
1.5. This policy sets out the rules that you must comply with to ensure that the system works effectively for everyone.

Privacy

1.6. The GDPR and Data Protection Act 2018 require all personal and special category data to be processed with the utmost credibility, integrity and accuracy. This applies to all data the school stores on its network regarding staff, pupils and other persons it deals with whilst carrying out its functions.
1.7. The school will only process data in line with its lawful basis to uphold the rights of both pupils and staff and other third parties.
1.8. In order to protect pupils' safety and wellbeing, and to protect the school from any third party claims or legal action against it, the school may view any data, information or material on the school's ICT systems (whether contained in an email, on the network, notebooks or laptops) and in certain circumstances, disclose that data, information or material to third parties, such as the police or social services. The school's Privacy Notice details the lawful basis under which the school is lawfully allowed to do so.
1.9. The school disclaimer that automatically appears at the end of each of your emails notifies the recipient that any email correspondence between you may be monitored. You must not remove this disclaimer. You should bring to the attention of any person who wishes or intends to send you an email that the school may monitor the content of their email.

General code of practice

The school's philosophy	In using ICT, you will follow the school's ethos and consider the work and feelings of others. You must not use the system in a way that might cause annoyance or loss of service to other users.
User ID and password and logging on	You will be given your own user ID and password. You must keep these private and not tell or show anyone what they are. Your password must be changed to your own once a generic password has been issued to you. If you forget or accidentally disclose your password to anyone else, you must report it immediately to a member of the ICT support staff. You must not use another person's account or allow another person to use your account. The facilities are allocated to you on a personal basis and you are responsible for the use of the machine when you are logged on. The school's system records and senior ICT staff monitor your use of the system both on and off the school premises. Use of the school's facilities by a third party using your username or password will be attributable to you, and you will be held accountable for the misuse.
Printing	The school may wish to check that expensive resources are being used efficiently and the member of staff may suggest other strategies to you to save on resources.
Locking/Logging off	You must log off from the computer you are using at the end of each of your sessions and wait for the standard login screen to reappear before leaving. This signals to the system that you are no longer using the service; it ensures security and frees up resources for others to use. When leaving your machine unattended you must lock your device using the Windows Key + L. Your machine must not be left unlocked when not in use.

Access to information not normally available	You must not use the system or the internet to find or use facilities or flaws in the system that might give access to information or areas of the network not normally available. You must not attempt to install software to explore or harm the system. Use of hacking tools, e.g. 'loggers', 'sniffers' or 'evidence elimination software', is expressly forbidden.
Connections to the system	You must not connect any personal devices hardware which may be detrimental to the school's network. Personal devices should only be connected to the school network at the discretion of the head teacher. This includes personal mobiles phone and tablets.
Connections to the computer	You should use the keyboard, mouse and any headphones provided. You must not adjust or alter any settings or switches without first obtaining the permission of a member of the ICT staff. You must never attempt to use any of the connectors on the back of any desktop computer, without permission from the ICT staff. You are not permitted to connect anything else to the computer without first getting the permission of a member of the ICT staff.
Virus	If you suspect that your computer has a virus, if must be switched off and you must report it to a member of the ICT technician as a matter of urgency.
Installation of software, files or media	You must not install or attempt to install software of any kind to network drives or local hard drives of networked desktop computers with the exception of installing operating system updates when requested to do so. You must not alter or re-configure software on any part of the school's system.
File space	You must manage your own file space by deleting old data rigorously and by deleting emails that you no longer require. Data relating to personnel or pupils should not be kept for longer than necessary.

Reporting faults, damage and malfunctions	You must report any faults, damage or malfunctions by email to the ICT technician, including full details and all error messages, as soon as possible.
Food and drink	You must not eat or drink, or bring food or drink, including sweets and chewing gum, into the Digital Den (Computer Room). You must always maintain a clean and quiet working environment.
Copying and plagiarising	You must not plagiarize or copy any material which does not belong to you.
Encryption	You must ensure that your laptop is encrypted before it leaves the school premises for the first time. (Staff can check this by making sure there is a padlock symbol over the 'C' drive on their laptop). Tablets must be passcode locked before leaving school premises. If personal mobile devices are used to collect school emails, you must ensure your device is passcode protected.
Copies of important work	It is your responsibility to keep paper copies and/or back-up copies, of important work as a secondary measure. Any data containing personal and special category data must not be stored on unencrypted media and paper back-ups must be stored in a secure lockable location.
Sharing Devices	School devices have been issued for your sole use. Do not share the devices among friends or family. Partners, children, other members of family and friends are not authorised to use any school device. This includes the actual device itself as well the sharing any passwords or urls.
Remote Access	From time to time the ICT support team will require remote access to your laptop. This could be to urgently address security issues, to install important updates or to address an ICT related issue. You will be advised of this via email or on-screen message before access is attempted. Failure to allow the support team access when required may results in your laptop being disabled as a security precaution.

Internet code of practice

1.10. The school can provide access to the internet from desktop PCs via the computer network and through a variety of electronic devices connected wirelessly to the network.
1.11. Whenever accessing the internet using the schools or personal equipment you must observe the code of practice below.
1.12. This policy and code of practice is designed to reduce and control the risk of offences being committed, liabilities being incurred, staff or other pupils being offended and the school's facilities and information being damaged.
1.13. Any breach of this policy and the code of practice will be treated extremely seriously, and it may result in disciplinary or legal action or expulsion.
1.14. The school may take steps, including legal action where appropriate, to recover from an individual any expenses or liabilities the school incurs because of the breach of this policy and code of practice.

Why is a code of practice necessary?

There are four main issues:

- Although the internet is often described as 'free', there is a significant cost to the school for using it. This cost includes telephone line charges, subscription costs (which may depend on how much a service is used) and the computer hardware and software needed to support internet access.
- Although there is much useful information on the internet, there is a great deal more material which is misleading or irrelevant. Using the internet effectively requires training and self-discipline. Training is available on request from ICT staff.
- Unfortunately, the internet carries a great deal of unsuitable and offensive material. It is important for legal reasons, reasons of principle, and to protect the staff and pupils who access to the internet, that it is properly managed. Accessing certain websites and services, and viewing, copying or changing certain material, could amount to a criminal offence and give rise to legal liabilities.
- There is a danger of importing viruses on to the school's network, or passing viruses to a third party, via material downloaded from or received via the internet, or brought into the school on disks or other storage media.

Internet code of practice

Use of the internet	The Internet should not normally be used for private or leisure purposes; it is provided primarily for education or business use. You may use the internet for other purposes provided that: • Such use is occasional and reasonable. • Such use does not interfere in any way with your duties; and • You always follow the code of practice. • You are aware that your internet activity is logged and could be monitored at any time and location, by senior staff.
Inappropriate material	You must not use the internet to access any newsgroups, links, list-servers, web pages or other areas of cyberspace that could be offensive because of pornographic, indecent, racist, violent, illegal, illicit, or other inappropriate content. "Inappropriate" in this context includes material which is unsuitable for viewing by pupils. You must not carry out any activity which defames or disparages the school, or risks bringing the school into disrepute. You are responsible for rejecting any links to such material which may appear inadvertently during research. If you encounter any material which could be regarded as offensive you must leave that website or service immediately and not make any copy of that material. If you encounter any difficulty in leaving a website or service, you must inform the ICT support staff immediately.
Misuse, abuse and access restrictions	You must not misuse or abuse any website or service or attempt to bypass any access controls or restrictions on any website or service.
Monitoring	The internet access system used by the school maintains a record which identifies who uses the facilities and the use that you make of them. The information collected includes which website and services you visit, how long you remain there and which material you

	view. This information may be analysed and retained, and it may be used in disciplinary and legal proceedings. This system also monitors the use of 'trigger words' which are deemed inappropriate. The system will keep a log of this information along with screen shots showing the context of the use of the words. Alerts relating to the use of trigger words will be sent to designated members of staff, who will follow them up as deemed necessary. Alerts will be sent as follows: • Pupils alerts will be monitored by ICT Support Staff and the Deputy Head; • Staff (including the head teacher) alerts will be monitored by the Deputy Head and ICT Support Staff; • The Deputy Head alerts will be monitored by the Head teacher and ICT Support Staff.
Giving out information	You must not give any information concerning the school, its pupils or parents, or any member of staff when accessing any website or service. This prohibition covers the giving of names of any of these people – the only exception being the use of the school's name and your name when accessing a service which the school subscribes to. You must not share any confidential information about the school its pupils or other members of the school community.
Personal safety	You should take care with who you correspond with. You should not disclose where you are or arrange meetings with strangers you have got in contact with over the internet. Do not give out your personal address.
Hardware and software	You must not make any changes to any of the school's hardware or software. This prohibition also covers changes to any of the browser settings. The settings put in place by the school are an important part of the school security arrangements and making any changes, however innocuous they might seem, could allow hackers and computer viruses to access or damage the school's systems. All laptops are installed with Anti-virus software. Please follow

	any directions given by the Anti-Virus (Sophos). If in doubt please contact ICT Support.
Copyright	You should assume that all material on the internet is protected by copyright and must be treated appropriately and in accordance with the owner's rights. You must not copy, download or plagiarise material on the internet unless the owner of the website expressly permits you to do so.

Email code of practice

1.15. The school's computer system enables members of the school to communicate by email with any individual or organisation with email facilities throughout the world.

1.16. For the reason outlined above, it is essential that a written policy and code of practice exists, which sets out the rules and principles for use of email by all.

1.17. Any breach of this policy and code of practice will be treated seriously and it may result in disciplinary or legal action or expulsion.

1.18. The school may take steps, including legal action where appropriate, to recover from an individual any expenses or liabilities the school incurs because of the breach of this policy and code of practice.

Email code of practice

Purpose	You should only use the school's email system for work related emails.
School's email disclaimer	The school's email disclaimer is automatically attached to all outgoing emails, you must not cancel or disapply it.
Monitoring	The frequency and content of incoming and outgoing external emails are checked to determine whether the email system is being used in accordance with this policy and code of practice. Senior members of staff have the ability to monitor emails and their content at all times and locations.

Security	As with anything else sent over the internet, emails are not completely secure. There is no proof of receipt, emails can be 'lost', they can suffer from computer failure and a determined 'hacker' could intercept, read and possibly alter the contents. As with other methods of written communication, you must make a judgment about the potential damage if the communication is lost or intercepted. Never send bank account information, including passwords, by email.
Program files and non-business documents	You must not introduce program files or non-business documents from external sources on to the school's network. This might happen by opening an email attachment or by downloading a file from a website. Although virus detection software is installed, it can never be guaranteed 100 percent successful, so introducing non-essential software is an unacceptable risk for the school. If you have any reason for suspecting that a virus may have entered the school's system, you must contact the ICT support staff immediately.
Quality	Emails constitute records of the school and are subject to the same rules, care and checks as other written communications sent by the school. Emails will be checked under the same scrutiny as other written communications. Staff members should consider the following when sending emails: • Whether it is appropriate for material to be sent to third parties • The emails sent and received may have to be disclosed in legal proceedings • Whether any authorisation is required before sending • Printed copies of some emails may be appropriate to retain in the same way as other correspondence, e.g. letter • The confidentiality between sender and recipient • Transmitting the work of other people, without their permission, may infringe copyright laws. • The sending and storing messages or attachments containing statements which could be construed as abusive,

	libelous, harassment may result in disciplinary or legal action being taken. • Sending or storing messages or attachments containing statements which could be construed as improper, abusive, harassing the recipient, libelous, malicious, threatening or contravening discrimination legislation or detrimental to the is a disciplinary offence and may also be a legal offence.
Inappropriate emails or attachments	You must not use email to access or send offensive material, chain messages or list-servers or for the purposes of bullying, intimidating or plagiarising work. You must not send personal or inappropriate information by email about yourself, other members of staff, pupils or other members of the school community. If you receive any inappropriate emails or attachments you must report them to technical staff.
Viruses	If you suspect that an email has a virus attached to it, you must inform the technical staff immediately.
Spam	You must not send spam (sending the same message to multiple email addresses) without the permission of senior staff.
Storage	You are advised to regularly delete material you no longer require and to archive material that you wish to keep.
Message size	If you wish to distribute files within the school, you can do so by using shared areas. A restriction is placed upon the size of attachments being sent.
Confidential Emails	You must ensure that confidential emails are always suitably protected. If working at home or remotely, you should be aware of the potential for an unauthorised third party to be privy to the content of the email. Confidential emails should be deleted when no longer required.

Emails – advice to staff

1.19. Staff should also be guided by the following good practice:

- Staff should check their emails daily and respond, as appropriate, within a reasonable period if the email is directly addressed to them.
- Staff should avoid spam, as outlined in this policy.
- Staff should avoid using the email system as a message board and thus avoid sending trivial global messages.
- Whilst accepting the convenience of the staff distribution list, staff should try to restrict its use to important or urgent matters.
- Staff should send emails to the minimum number of recipients.
- Staff are advised to create their own distribution lists, as convenient and appropriate.
- Staff should always include a subject line.
- Staff are advised to keep old emails for the minimum time necessary.

Further guidelines for use of email

1.20. Remember – emails remain a written record and can be forwarded to others or printed for formal use.

1.21. As a rule of thumb, staff should be well advised to only write what they would say face to face and should avoid the temptation to respond to an incident or message by email in an uncharacteristic and potentially aggressive fashion.

1.22. Remember, “tone” can be misinterpreted on the printed page and once it is sent it could end up in the public domain forever. Email lacks the other cues and clues that convey the sense in which what you say is to be taken, and you can easily convey the wrong impression.

1.23. Remember that sending emails from your school account is similar to sending a letter on school letterhead, so don't say anything that might bring discredit or embarrassment to yourself or the school.

1.24. Linked with this and given the popularity and simplicity for recording both visual and audio material, staff are advised to remember the possibility of being recorded in all that they say or do.

Social Media Code of Practice

1.25. The school recognises that the internet provides unique opportunities to participate in interactive discussions and share information on particular topics using a wide range of social media. However, employees’ use of social media can pose risks to confidentiality and intellectual property, the school’s reputation and can jeopardise compliance with legal obligations

1.26. Employees must be conscious at all times of the need to keep their personal and professional lives separate.

Overarching Principles:

- You should not put yourself in a position where there is a conflict between your work for the school and your personal interests.
- You must not engage in activities involving social media which might bring the school into disrepute.
- You must not represent your personal views as those of the school on any social medium.
- You must not discuss personal information about pupils, other school employees or professionals you interact with as part of your job on social media.
- You must not use social media and the internet in any way to attack, insult, and abuse or defame pupils, their family members, colleagues, other professionals, other organisations or the school.
- You must be accurate, fair and transparent when creating or altering online sources of information on behalf of the school or the LA.
- You must ensure, when contacting students for school business, appropriate monitored resources i.e., school mobile phone, school email system etc. are used as a safeguarding measure.

1.27. Personal Use of social media

- Employees must not identify themselves as employees of the school in their personal web space. This is to prevent information on these sites from being linked with the school and to safeguard the privacy of staff members, particularly those involved in providing sensitive frontline services.
- The school does not expect employees to discontinue contact with their family members via personal social media once the school starts providing services for them. However, any information employees obtain in the course of their employment must not be used for personal gain or be passed on to others who may use it in such a way.
- Employees must not have any contact with pupils' family members through personal social media if that contact is likely to constitute a conflict of interest or call into question their objectivity.
- Employees must decline 'friend requests' from pupils they receive in their personal social media accounts.
- Information employees have access to as part of their employment, including personal information about pupils and their family members, colleagues, LA staff and other parties and school or LA corporate information must not be discussed on their personal web space.
- Photographs, videos or any other types of images of pupils and their families or images depicting employees wearing clothing with school logos on must not be published on personal web space.

- School email addresses and other official contact details must not be used for setting up personal social media accounts or to communicate through such media.
- The school only permits limited personal use of social media during designated break points. However, employees are expected to devote their contracted hours of work to their professional duties, and, in practice, personal use of the internet should not be in the school's time. Any such use should not:
    - Deprive pupils of the use of the equipment and/or
    - Interfere with the proper performance of employee's duties

- Caution is advised when inviting work colleagues to be 'friends' in personal social networking sites. Social networking sites blur the line between work and personal lives, and it may be difficult to maintain professional relationships or it might be just too embarrassing if too much personal information is known in the work place.

- Employees are advised that they set the privacy levels of their personal sites as strictly as they can and to opt out of public listings on social networking sites to protect their own privacy. Employees should keep their passwords confidential, change them often and be careful about what is posted online. It is not appropriate to reveal home addresses, telephone numbers and other personal information. It is a good idea to use a separate email address just for social networking so that any other contact details are not given away.

- If a message is received on their social networking profile that they think could be from a pupil or parent they should report it to the Head Teacher so that this can be investigated, and appropriate action taken.

- Employees should not make defamatory remarks about school / colleagues / pupils / parents or the Local Authority or post anything that could potentially bring the school or Local Authority into disrepute.

1.28. Using Social Media on Behalf of the School

- Employees can only use official school sites for communicating with pupils or to enable pupils to communicate with one another. Employees should seek permission from the Head Teacher before creating an official school site explaining their business reasons for doing so.
- You must use an official school email address when signing up for any account so that the account is not specially linked to any one member of staff.
- Use an approved version of the school logo as the profile picture.
- Refrain from using a picture of pupil on areas that can be publicly seen e.g. the profile and cover pictures, unless express parental consent is provided.
- Create a strong password that cannot be easily guessed.
- Ensure that information regarding passwords for school social media accounts is not shared with anyone other than designated staff members.
- Do not include the full names of any pupils or staff.

- Check the backgrounds of photos to ensure that they are appropriate for publication on the school website and do not include the full faces of pupils for whom parental consent has not been obtained.
- Ensure there is no link to any personal social media account or contact details anywhere on the account
- Ensure that passwords are changed when necessary, including:
  - When staff members with access to the accounts leave the school
  - When a staff member previously responsible for the accounts no longer has responsibility.
  - In the event that the security of the account is breached. e.g. if a pupil gains access to the accounts
- If you are contacted for comments about the school for publication anywhere, including in any social media outlet please direct the enquiry to the Head Teacher.
- Any official school sites created must not breach the terms and conditions of social media service providers, particularly with regard to minimum age requirements. Employees must, at all times, act in the best interests of children and young people when creating, participating in or contributing content to social media sites.
- While communicating on the school social media account, employees must::

  - Be respectful, polite and positive.
  - Express gratitude for positive posts.
  - Answer questions helpfully and in as much detail as is necessary.
  - Use user-friendly language and avoid wording that is inaccessible to those following the account, e.g. industry jargon.
  - Avoid directly tagging any individuals in the content of posts.
  - Avoid direct messaging with pupils under all circumstances.
  - Avoid direct and private messaging with parents aside from circumstances where it is appropriate, e.g. in response to a direct query.
  - Only interact with politically neutral posts and posts from reputable and neutral sources.

1.29. Monitoring school social media accounts

- Employees must ensure that the social media account remains a positive, neutral environment which represents the values and ethos of the school.

Any member of staff monitoring Social Media accounts will ensure that posts from others are removed if they:

- Are abusive.
- Include identifying information about pupils or staff.
- Use bad or inappropriate language.
- Have controversial opinions attached to them that may be construed as offensive.
- Raise complaints or concerns about specific staff members.
- Engage in rumours or gossip, whether negative or positive, about the personal lives of staff members, pupils, or parents of pupils.
- If a post is removed, employees will ensure that the poster is told why this decision was made to avoid repeat issues or consequent complaints.

Mobile devices

1.30. Employees may only use school-owned mobile devices for educational purposes.
1.31. Employees must only use personal mobile devices during out-of-school hours, including break and lunch times unless authorisation has been sought by a member of the Leadership Team.
1.32. Employees must ensure that personal mobile devices are either switched off or set to silent mode during school hours and will only make or receive calls when there are no pupils in the same room.
1.33. Employees must ensure that personal mobile devices are not visible to pupils, and are stored in a lockable cupboard or personal bag during lesson times.
1.34. Employees must ensure that images or videos taken on school mobile devices are only for the purpose of teaching and learning.
1.35. Employees must ensure that any images or video recordings are transferred to the computer and deleted from the device by the end of the working week.
1.36. Employees must not use mobile devices to send inappropriate messages, images or recordings.
1.37. Employees must ensure that personal and school-owned mobile devices do not contain any inappropriate or illegal content.
1.38. Employees must not access the school's WiFi network using personal mobile devices, unless permission has been given by the Headteacher.
1.39. Employees must not use personal mobile devices to communicate with pupils or parents, except by telephone, and only if their phone number is withheld.
1.40. Employees must not store any images or videos of pupils, staff or parents on any mobile device unless consent has been sought from the individual(s) in the images or videos.
1.41. In line with the above, employees must only process images or videos of pupils, staff or parents for the activities for which consent has been sought.

Working from home

1.42. Employees must adhere to the principles of the GDPR when taking work home.
1.43. Employees must ensure they obtain permission from the Headteacher before any personal data is transferred from a school-owned device to a personal device.
1.44. Employees must ensure any data transferred from a school-owned device to a personal device is encrypted.
1.45. Employees must ensure any sensitive persona data is not transferred to a personal device unless completely necessary – and, when doing so, that it is encrypted.
1.46. Employees must act in accordance with the school's Online Safety Policy when transporting school equipment and data.

Training

1.47. Employees must ensure they participate in any online safety training offered to them and will remain up-to-date with current developments in social media and the internet as a whole.
1.48. Employees must allow the Designated Safeguarding Lead to undertake regular audits to identify any areas of need they may have in relation to training.
1.49. Employees must ensure they employ methods of good practice and act as a role model for pupils when using the internet and other digital devices.
1.50. Employees must ensure that they deliver any training or teaching to pupils as required.

Reporting misuse

1.51. Employees must adhere to any responsibility they have for monitoring, as outlined in the Online Safety Policy, e.g. to monitor pupils' internet usage. Employees must report any misuse by pupils to ICT Support staff or the DSL; any misuse by staff members should be reported to the Deputy Head or Head Teacher.
1.52. Employees must understand that their use of the internet will be monitored in line with this agreement, and recognise that if they breach the terms of this agreement they may face disciplinary action.
1.53. Any staff involved in monitoring pupil or staff use of ICT must only do so in line with the expectations set out in this Acceptable Use Policy; and if they have reason to believe that this policy has been breached, and not for any other purpose.

Signing this ICT Acceptable Use Policy

Employees will be required to read and follow this agreement, and sign to say they accept its contents.

I confirm that I have read and understand this policy; I know what my responsibilities are within it; and I agree to abide by it.

I understand that the Headteacher may decide to take disciplinary action against me in accordance with the Disciplinary Policy and Procedures, if I breach this policy.

I confirm that I am aware that all my electronic communications on school devices, including emails and website searches and visits may be monitored by identified members of staff, as set out in this agreement, and that this applies even if I am working from home.

Signed: _____ Date: _____

Print name: _____

Position: _____

Annex 1: Pupil Acceptable Use Policy

Pupil ICT Acceptable Use Agreement

At St Stephen's Primary School, we know that it can be fun to use technology as part of your learning experience. We want everyone to be able to use technology, like computers, laptops and tablets, but it is important that you are safe when you are using them.

We have created this agreement to help you understand how to be safe when you are using technology. Please read this carefully to understand what is acceptable use of ICT and computing equipment. Ask a trusted adult if there is something that you do not understand.

Parents – please read through this agreement with your child at home, help them to understand it, and keep it at home. We have also spoken with children about it in school.

I will:

- ✓ Only use technology, such as a computer, when a teacher has given me permission.
- ✓ Only use technology for the reason I have been asked to use it.
- ✓ Only use the internet when an adult has given me permission.
- ✓ Ask for help when I have a problem using the technology.
- ✓ Look after the device and try not to damage it.
- ✓ Tell an adult if my device is not working or damaged.
- ✓ Tell an adult if I think someone else is not using technology safely or correctly.
- ✓ Tell a trusted adult if I see something online that makes me upset or I think is inappropriate.
- ✓ Tell a trusted adult if I have any worries about online safety, from home or school.

I will not:

- Tell another pupil my username and password.
- Share personal information, such as my age and where I live, about myself or my friends online.
- Access social media, such as TikTok, Snapchat or Facebook using a school device.
- Send messages to strangers on the internet.
- Take photos of myself or my friends using a school device, unless an adult in school has told me I can.

We expect all pupils to be able to accept the points below.

- ☐ I understand why it is important to use technology safely and correctly.
- ☐ I understand my responsibilities when using technology.
- ☐ I understand that I may not be allowed to use technology if I do not use it safely and correctly.
- ☐ I will follow these rules at all times.

Parents – please read these expectations with your child and double-check they understand them.

Please contact a member of staff if you are worried about your child's safety online.