ST JAMES' RC PRIMARY SCHOOL

ONLINE SAFETY AND ACCEPTABLE USE POLICY

This policy has the school values at its heart:

Faith in action,

Working together,

Walking in the footsteps of Christ

Our Vision is:

Share our love of God every day in all that we learn, do and say.

Development of this Policy

This on line safety policy has been developed by the e- safety Subject Leader and staff.

Should serious e-safety incidents take place, the following people should be informed:	The Headteacher, the DSL and the e-safety Subject Leader.

The school will monitor the impact of the policy using:

- Logs and responses of reported incidents
- Monitoring logs of internet activity (including sites visited in planning)
- Surveys / questionnaires of pupils, parents and staff.

The purpose of this policy is to:

- Ensure the safety and wellbeing of children is paramount when adults and children are using the internet, social media or mobile devices
- Provide staff and volunteers with the overarching principles that guide our approach to online safety
- Ensure that, as an organisation, we operate in line with our values and within the law in terms of how we use online devices

This policy applies to all members of the school community (including staff, learners, governors, volunteers, parents and carers, visitors and community users) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed).

Roles and Responsibilities:

The Head teacher, E-Safety Subject Leader and Governors will ensure that:

- The policy is reviewed annually or whenever the need arises;
- Appropriate response is given to any e-safety incident;
- There is overall management of e-safety within school;
- They keep up to date with emerging risks and threats through technology use;
- E-safety is observed in all aspects of technology within school (ICT suite, laptops, ipads, cameras);
- E-safety incidents are recorded on cpoms;

- They receive relevant and regularly updated training on online safety to enable them to understand the risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online;
- Meet regularly with the online safety governor to discuss current issues, review (anonymised) incidents and filtering and monitoring logs and ensure that annual (at least) filtering and monitoring checks are carried out.

Governors will ensure that

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy.

A member of the Governing Body will take on the role of Online Safety Governor to include:

- Regular meetings with the E-Safety Subject Leader;
- Regularly receiving (collated and anonymised) reports of online safety incidents:
- Checking that provision outlined in the Online Safety Policy e.g. online safety education provision and staff training is taking place as intended;
- Ensuring that the filtering and monitoring provision is reviewed and recorded, at least annually.

The Network Manager (SNS) is responsible for ensuring that:

- The school's technical infrastructure is secure and is not open to misuse or malicious attack;
- The school meets the required e-safety technical requirements;
- Users may only access the networks and devices through properly enforced password protection, in which passwords are regularly changed;
- They keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant;
- The use of the network/internet is regularly monitored in order that any misuse/attempted misuse can be reported to the Head teacher and E-Safety Subject Leader for investigation/action;
- Monitoring software/systems are implemented and updated as agreed in school policies.

All staff are responsible for ensuring that:

- They have an up to date awareness of e-safety matters and of the current school e-safety policy and practices;
- They have read, understood and signed the Staff Acceptable Use Agreement;
- They report any suspected misuse or problem to the Head teacher, the e-Safety Subject Leader and the Designated Safeguarding Lead;
- All digital communications with pupils and parents should be on a professional level and only carried out using official school systems;
- Comments posted on Seesaw will be in alignment with this policy;
- E-safety issues are embedded in all aspects of the curriculum and other activities;
- Pupils understand and follow the e-safety and acceptable use agreements;
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;

- They monitor the use of digital technologies, ipads, laptops, computers, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices;
- In lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches;
- All websites used in school and for remote learning have been pre-visited by the Class Teacher to ensure that they are appropriate;
- When using Zoom for remote learning all aspects of this policy are followed. For more information regarding Home Learning/Online Teaching please see the relevant policies.

The Designated Safeguarding Lead has overall responsibility for e-safety and should be trained in e-safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from:

- Sharing of personal data;
- Access to illegal/inappropriate materials;
- Inappropriate on-line contact with known adults/strangers;
- Potential or actual incidents of grooming;
- Cyber-bullying.

Pupils will ensure that:

- They are responsible for using the all-digital technology systems in accordance with the Pupil Acceptable Use Policy;
- They have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- They understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so;
- They understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the On-line Safety Policy is applicable wherever they are using technology.

In addition, Year 6 will be expected to know and understand policies on the use of mobile devices in school.

All Parents will ensure that:

They support the school in promoting good e-safety practice and follow guidelines on the appropriate use of digital and video images taken at school events.

The school will take every opportunity to help parents understand e-safety issues through curriculum evenings, newsletters, letters and the website.

Community users will ensure that:

Community users such as the PTA and who access school systems/website/learning platform as part of the wider school provision will be expected to sign a community user Aceeptable User Agreement before being provided with access to school systems. The community user's acceptable use agreement template can be found in the school office.

Teaching and Learning

Why the internet use is so important.
The internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide children with quality internet access as part of their learning experience. Internet use is a part of the statuatory curcculum and a necessary tool for staff and pupils.
Internet use will enhance learning.
The school internet access is designed expressly for pupil use and includes filtering appropariate to the age of pupils. Pupils will be taught what internet use is accetable and what is not and will be given clear objectives for internet use. Pupils will be educated in the effective use of the internet in reasearch, including the skills of knowledge locataion, retreival and evaluation.
Pupils will be taught how to evaluate internet content.
The school will ensure that the use of internet derived materials by staff and pupils complies with copyright law. Pupils should be taught to be critically aware of the materials they read an shown how to validate information before accepting its accuracy.

Bring Your Own Device (BYOD)

The educational opportunities offered by mobile technologies are being expanded as a wide range of devices, software and online services become available for teaching and learning, within and beyond the classroom. This has led to the exploration by schools of users bringing in their own technologies in order to provide a greater freedom of choice and usability. However, there are a number of e-safety considerations for BYOD. Use of BYOD should not introduce vulnerabilities into existing secure environments. Please see the Mobile Phone Policy for further details. Considerations will need to include: levels of secure access, filtering, data protection, storage and transfer of data, mobile device management systems, training, support, acceptable use, auditing and monitoring. The school has a policy that only Year 6 pupil may bring mobile phones to school but that they must remain in the school office and have no access to the internet.

- The school has a set of clear expectations and responsibilities for all users.
- The school adheres to GDPR principles.
- All users are provided with and accept the Acceptable Use Agreement.
- All network systems are secure and access for users is differentiated.
- Where possible devices will be covered by the school's normal filtering systems, while being used on the premises.
- All users will use their username and password and keep this safe.

Pupils receive training and guidance on the use of personal devices.

- Regular audits and monitoring of usage will take place to ensure compliance.
- Any device loss or theft will be reported.

Use of digital and video images:

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 and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying 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 advised that employers carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm.

When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites. These skills are explicitly taught during e safety sessions across the school.

In accordance with guidance from the Information Commissioner's Office, parents are welcome to take videos and digital images of their children at school events for their own personal use. To respect everyone's privacy and in some cases protection, as a school we instruct parents that these images should not be published/made publicly available on social networking sites, nor should parents comment on any activities involving other pupils in the digital/video images.

Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. These images should only be taken on school equipment. The personal equipment of staff should not be used for such purposes however in circumstances where no other technology is available devices can be used for photos only and all photos must be removed and deleted from devices and cloud storage before the device leaves school.

Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

Pupils must not take, use, share, publish or distribute images of others during school time without their permission.

Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.

Pupil's full names should not be used anywhere on a website, particularly in association with photographs.

Written permission from parents will be obtained before photographs of pupils are published on the school website through the Acceptable Use Contracts.

Social Media - Protecting Professional Identity:

All schools have a duty of care to provide a safe learning environment for pupils and staff. Schools could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school liable to the injured party. Reasonable steps to prevent predictable harm must be in place. The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions.
- Risk assessment, including legal risk.

School staff should ensure that:

- No reference should be made in social media to pupils, parents or school staff without their permission.
- They do not engage in online discussion on personal matters relating to members of the school community.
- Personal opinions should not be attributed to the school.
- No images of children in the school should be used (unless they are a direct relation such as their child.)
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

The school's use of social media for professional purposes will be checked regularly.

In the Event of Inappropriate Use

Should a child be found to misuse the online facilities whilst at school, the following consequences should occur:

If children accidentally access something inappropriate on the internet, the children know to immediately close the laptop or turn off the monitor of the desktop computer. They know to immediately tell a member of staff. Where appropriate, parents will be contacted to advise them.

All incidents will be recorded on cpoms.

Any child found to be misusing the internet by not following the Acceptable Use Agreement will have a letter sent home or a phone call to parents explaining the reason for suspending the child's use for a particular lesson or activity. Further misuse of the agreement may result in further sanctions which could include not being allowed to access the internet for a period of time.

Parents will be contacted outlining any breach where a child is deemed to have misused technology against another child or adult.

Children will be taught and encouraged to consider the implications for misusing the internet and posting inappropriate materials to websites, for example, as this may have legal implications.

Responding to incidents of misuse:

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities; in this case the Head teacher will contact the police.

Secure transfer of data and access out of school

The school recognises that personal data may be accessed by users out of school, or transferred to the LA or other agencies. In these circumstances users may not remove or copy sensitive or restricted or protected personal data from the school without permission and unless the media is encrypted and password protected and is transported securely for storage in a secure location. Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (e.g. family members) when out of school. When restricted or protected personal data is required by an authorised user from outside the organisation's premises (e.g. by a member of staff to work from their home), they should preferably have secure remote access to the management information system or learning platform. If secure remote access is not possible, users must only remove or copy personal or sensitive data from the organisation if the storage media, portable or mobile device is encrypted and is transported securely for storage in a secure location. Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software. Particular care should be taken if data is taken or transferred to another country.

Monitoring

The contents of our IT resources and communications systems are the school's property. Therefore, staff should have no expectation of privacy in any message, files, data, document, telephone conversation, social media post conversation or message, or any other kind of information or communications transmitted to, received or printed from, or stored or recorded on our electronic information and communications systems. The school reserves the right to monitor, intercept and review staff activities using our IT resources and communications systems, including but not limited to social media postings and activities, to ensure that our rules are being complied with and for legitimate business purposes and you consent to such monitoring by your acknowledgement of this policy and your use of such resources and systems. This might include, without limitation, the monitoring, interception, accessing, recording, disclosing, inspecting, reviewing, retrieving and printing of transactions, messages, communications, postings, log-ins, recordings and other uses of the systems as well as keystroke capturing and other network monitoring technologies. The school may store copies of such data or communications for a period of time after they are created, and may delete such copies from time to time without notice. All staff are advised not to use our IT resources and communications systems for any matter that he or she wishes to be kept private or confidential from the school.

Educational or Extra-Curricular Use of Social Media

If your duties require you to speak on behalf of the school in a social media environment, you must follow the protocol outlined below. The Head teacher may require you to undergo training before you use social media on behalf of the school and impose certain requirements and restrictions with regard to your activities. Likewise, if you are contacted for comments about the school for publication anywhere, including in any social media outlet, you must direct the inquiry to the Head Teacher.

Recruitment

The school will use internet searches to perform pre-employment checks on candidates in the course of recruitment. Where the school does this, it will act in accordance with GDPR and equal opportunities obligations.

Responsible use of Social Media

The following sections of the policy provide staff with common-sense guidelines and recommendations for using social media responsibly and safely.

Photographs for use of Social Media

Any photos for social media posts may only be taken using school cameras/devices or devices that have been approved in advance by the Head teacher. Where any device is used that does not belong to the school all photos must be deleted immediately from the device and any other platform (e.g. cloud) once the photos have been uploaded to a device belonging to the school.

Staff Protocol for use of Social Media

Where any post is going to be made on the school's own social media the following steps must be taken:

- Ensure that permission from the child's parent has been sought before information is used on social media.
- Ensure that there is no identifying information relating to a child/children in the post – e.g. any certificates in photos are blank/without names or the child's name cannot be seen on the piece of work.
- The post must be a positive and relate to any achievements.
- Social Media can also be used to issue updates or reminders to parents and the Head teacher will have overall responsibility for this. Should you wish for any reminders to be issued you should contact the Head teacher to ensure that the post can be issued.
- The proposed post must be presented to the Head teacher for confirmation that the post can 'go live' before it is posted on any social media site.
- The Head teacher will post the information, but all staff have responsibility to ensure that the Social Media Policy has been adhered to.

Protecting our business reputation

Staff must not post disparaging or defamatory statements about:

- The school;
- Current, past or prospective staff*;*
- Current, past or prospective pupils*;*
- Current, past or perspective families;
- The school's suppliers and services providers;
- Other affiliates and stakeholders.

Staff should avoid social media communications that might be misconstrued in a way that could damage the school's reputation, even indirectly. If staff are using social media they should make it clear in any social media postings that they are speaking on their own behalf. Staff should write in the first person and use a personal rather than school e-mail address when communicating via social media. Staff are personally responsible for what they communicate in social media. Staff should remember that what they publish might be available to be read by the masses (including the school itself, future employers and social acquaintances) for a long time. Staff should keep this in mind before they post content. If staff disclose whether directly or indirectly their affiliation to the school as a member of staff whether past, current or prospective, they must also state that their views do not represent those of the school. Staff must ensure that their profile and any content posted are consistent with the professional image they are required to present to colleagues, pupils and parents. Staff must avoid posting comments about confidential or sensitive school related topics.

Even if staff make it clear that their views on such topics do not represent those of the school, such comments could still damage the school's reputation and incur potential liability. If a member of staff is uncertain or concerned about the appropriateness of any statement or posting, they should refrain from making the communication until he or she has discussed it with the Head teacher. If a member of staff sees content in social media that disparages or reflects poorly on the school, it's staff, pupils, parents, service providers or stakeholders, they are required to report this in the first instance to the Head Teacher without delay. All staff are responsible for protecting the school's reputation.

Respecting intellectual property and confidential information

Staff should not do anything to jeopardise school confidential information and intellectual property through the use of social media. In addition, staff should avoid misappropriating or infringing the intellectual property of other schools, organisations, companies and individuals, which can create liability for the School, as well as the individual author. Staff must not use the school's logos, brand names, slogans or other trademarks, or post any of our confidential or proprietary information without express prior written permission from the Head teacher. To protect yourself and the school against liability for copyright infringement, where appropriate, reference sources of particular information you post or upload and cite them accurately. If you have any questions about whether a particular post or upload might violate anyone's copyright or trademark, ask the Head teacher in the first instance before making the communication.

Respecting colleagues, pupils, parents, clients, service providers and stakeholders

Staff must not post anything that their colleagues, the school's past, current or prospective pupils, parents, service providers or stakeholders may find offensive, including discriminatory comments, insults or obscenity. Staff must not post anything related to colleagues, the school's past, current or prospective pupils, parents, service providers or stakeholders without their advanced written permission.

Reporting and responding

The 2021 Ofsted "Review of Sexual Abuse in Schools and Colleges" highlighted the need for schools to understand that reporting systems do not always respond to the needs of learners. While the report looks specifically at harmful sexual behaviours, schools may wish to address these issues more generally in reviewing their reporting systems. The Ofsted review suggested:

"School leaders should create a culture where sexual harassment and online sexual abuse are not tolerated, and where they identify issues and intervene early to better protect children and young people. ..In order to do this, they should assume that sexual harassment and online sexual abuse are happening in their setting, even when there are no specific reports, and put in place a whole-school approach to address them. This should include routine record-keeping and analysis of sexual harassment and sexual violence, including online, to identify patterns and intervene early to prevent abuse"

The school will take all reasonable precautions to ensure online safety for all school users but recognises that incidents may occur inside and outside of the school (with impact on the school) which will need intervention. The school will ensure that:

- There are clear reporting routes which are understood and followed by all members of the school community which are consistent with the school safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies.
- All members of the school community will be made aware of the need to report online safety issues/incidents.
- Reports will be dealt with as soon as is practically possible once they are received.
- The Designated Safeguarding Lead, e Safety Subject Lead and other responsible staff have appropriate skills and training to deal with online safety risks.
- If there is any suspicion that the incident involves any illegal activity or the potential for serious harm the incident must be escalated through the agreed school safeguarding procedures, this may include:
    - Non-consensual images
    - Self-generated images
    - Terrorism/extremism
    - Hate crime/ Abuse
    - Fraud and extortion
    - Harassment/stalking
    - Child Sexual Abuse Material (CSAM)
    - Child Sexual Exploitation Grooming
    - Extreme Pornography
    - Sale of illegal materials/substances
    - Cyber or hacking offences under the Computer Misuse Act
    - Copyright theft or piracy

Any concern about staff misuse will be reported to the Headteacher, unless the concern involves the Headteacher, in which case the complaint is referred to the Chair of Governors and the local authority.

Where there is no suspected illegal activity, devices may be checked using the following procedures:

- One or more senior members of staff should be involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated device that will not be used by learners and, if necessary, can be taken off site by the police should the need arise (should illegal activity be subsequently suspected). Use the same device for the duration of the procedure.
- Ensure that the relevant staff have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed, and attached to the form
- Once this has been completed and fully investigated the senior members of staff will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
    - internal response or discipline procedures

  - involvement by local authority
  - police involvement and/or action

It is important that those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively and that there are support strategies in place such as peer support for those reporting or are affected by an online safety incident. incidents should be logged on cpoms. Relevant staff are aware of external sources of support and guidance in dealing with online safety issues such as the local authority, police, CEOP. Those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions as relevant.

Learning from the incident or the pattern of incidents will be provided (as relevant and anonymously) to:

- Staff, through regular briefings;
- Pupils, through assemblies and lessons;
- Parents, through newsletters, school social media, website;
- Governors, through regular safeguarding updates.

Social Media

We use X to share and showcase the wonderful things happening at St James' RC Primary School. X will not be used to engage with individual parents directly, however, important announcements and notices could be sent as part of general communication to parents.
To ensure online safety:

- The Head teacher is the only person who posts through the X handle.
- No photos or information that could identify a child ie. faces/names will be included on the X updates.
- The school will follow only educational users and not retweet any other tweets.

In order to safeguard the pupils no photos or names of pupils will be used. St James' RC Primary School seeks photographic consent of all the pupils. Any photographs of children will be the backs of their heads so they are unidentifiable.

Anyone can follow the school's X account. Regular checks will take place by the e safety Subject Leader to check recent followers. Any user following the school account that is deemed unsuitable or not adding any value to the school will be blocked. The Head teacher will make this decision on a case-by-case basis. Parents will be encouraged to follow the official school account to receive the information the school is posting up to X. We welcome the interactions of people on X however the following actions are inappropriate and will lead to an immediate blocking of the user:

- Offensive language or remarks aimed at the school, its staff, parents, governors or others affiliated with the school;
- Unsuitable images or content posted into its feed;
- Unsuitable images or content finding its way from another's account into school feed;
- Images or text that infringe upon copyright;
- Comments that aim to undermine the school, its staff, parents, governors or others affiliated with the school.

Any incidents of a serious nature may be reported to the relevant/appropriate authorities.

Acceptable Use

The School embrace the use of new and mobile technologies and acknowledge they are a valuable resource in the classroom having educational purpose. However, by accessing the school's systems and networks, it is likely that staff will use personal data and so must abide by the terms of the Data Protection Act 2018 when doing so including ensuring adequate security of that personal information. Staff's own personal devices will not be connected to the school's wifi. When in School staff should connect their device via the school's wireless network for security. When out of School, staff should access work systems on their mobile device using Lgfl Staffmail or their encoded memory sticks. This ensures a secure connection. All internet access via the network is logged and, as set out in the Acceptable Use Policy, employees are blocked from accessing certain websites whilst connected to the school network. The use of camera, microphone and/or video capabilities are prohibited whilst in school unless the device is a school device. Any pictures, videos or sound recordings can only be used for school purposes and cannot be posted or uploaded to any website or system outside of the School network. Staff must not use their device to take pictures/video/recordings of other individuals without their advance written permission to do so.

Non-Acceptable Use

Any apps or software that are downloaded onto the user's device whilst using the school's own network must be done by the school technician or the Computing Subject leader. Devices may not be used at any time to:

- Store or transmit illicit materials;
- Store or transmit proprietary information belonging to the school;
- Harass others;
- Act in any way against the School's acceptable use policy and other safeguarding and data related policies.

Technical support is not provided by the School on the user's own devices

Devices and Support

Smartphones including iPhones and Android phones are not allowed to access the school's wifi. Tablets including iPad and Android are allowed if they have been provided for the school, or if they are used for one of the school run clubs. At the clubs they must then be under constant supervision of the leading adult. Any new devices must be presented to the technician for proper job provisioning and configuration of standard apps, such as browsers, office productivity software and security tools, before they can access the network.

Security

In order to prevent unauthorised access, devices must be password/pin protected using the features of the device and a strong password is required to access the school network.

When using personal data, it is the user's responsibility to ensure they keep data secure on their device. This includes preventing theft and loss of data (for example through password protection and cloud back up) keeping information confidential (for example by ensuring access to emails or sensitive information is password protected) and maintaining that information.

The School does not accept responsibility for any loss or damage to the user’s device when used on the School’s premises. It is up to the user to ensure they have their own protection on their own device.

Staff are prevented from installing email apps which allow direct access to school emails without use of a login/password.

If information is particularly sensitive then users should ensure that the data is either appropriately secured or deleted from the device (including from any local copies which may have been stored on the device.)

In the event of any loss or theft of personal data, this must be reported immediately as a data breach in accordance with the school’s data breach policy.

The School may require access to a device when investigating policy breaches for example to investigate cyber bullying.

Staff are not permitted to share access details to the school’s network or Wi-Fi password with anyone else.

The School will not monitor the content of the user’s own device but will monitor any traffic over the School system to prevent threats to the School’s network.

Year 6 Mobile Phones

We accept that parents feel the need to give their children mobile phones to protect them from everyday risks involving personal security and safety. Permission to have a mobile device at school while under the school’s supervision is contingent on parent permission in the form of a signed copy of the Mobile Phone BYOD Form. Parents may revoke approval at any time. School administration may revoke approval due to improper use of technology. The school agrees that both home and school are responsible for teaching digital citizenship. At school, regular discussions regarding proper etiquette, safety and responsible use will be infused into the curriculum. Formal lesson plans regarding e Safety are taught within our Computing and RHE curriculum. Using mobile devices to bully and threaten is unacceptable and will not be tolerated. In some cases, it can constitute criminal behaviour. Depending on severity, the school reserves the right to withdraw the agreement to allow the pupil to bring the mobile device to school. The school accepts no responsibility for replacing lost, stolen or damaged mobile devices. It is the responsibility of pupils who bring mobile devices to school to abide by the guidelines outlined in this document.

Disclaimer

The School reserves the right to disconnect devices or disable services without notification. The employee is expected to use his or her devices in an ethical manner at all times and adhere to the school’s policy as outlined above. The employee is personally liable for all costs associated with his or her device. The school reserves the right to take appropriate disciplinary action up to and including summary dismissal for non-compliance with this policy.

Links with other policies

- Mobile phone policy
- Child protection and safeguarding policy

Monitoring

This policy will be updated in line with any new developments in the school and/or any new government guidance. This Policy will be renewed annually.

It was last reviewed in: spring 2024 It will next be reviewed in: spring 2025

This statement of policy was approved by the Governing Body at their meeting on:-

Date: ________________________________

Signed: _______________________________ (Chairperson)

____________________________________ (Head teacher)

St James' RC Primary School Acceptable Use Policy for Internet Access

As part of the school's continuing ICT development, we offer pupils of St. James' RC Primary access to facilities that include the Internet. Before being allowed to use the Internet, it is a statutory requirement that all pupils must obtain parental permission and both they and you must sign and return the enclosed form as evidence of your approval and their acceptance of the school rules on this matter.

Access to the Internet will enable pupils to explore thousands of websites throughout the world – an important interaction in this digital age. LGFL (London Grid for Learning) provides a filtered and secure intranet and provides us with a strict and secure Firewall but the nature of the Internet is such that sites which contain these sorts of materials are constantly changing which means that no filtering can be perfect. Whilst our aim for Internet use is to further education goals and objectives, pupils may find ways to access other material as well.

We believe that the benefits to pupils from access to the Internet exceed any disadvantages, although ultimately, parents and guardians of pupils are responsible for setting and conveying the standards that their children should follow when using media and information sources. To that end this school supports and respects each family's right to decide whether or not to allow their child access.

Staff will provide guidance to pupils so that they will be able to manage risks when they make use of telecommunications and electronic information sources to conduct research and other studies related to the curriculum. A member of staff will supervise pupils while they are using the Internet or email.

As much as possible, pupils will be directed to information resources that have been reviewed and evaluated prior to use. While pupils may be able to move beyond those resources to others that have not been evaluated by staff, they shall be provided with guidelines and lists of resources particularly suited to the learning objectives. All pupils are expected to follow staff instructions including the instruction of the After School Club staff. If a pupil does not follow these, they will no longer be allowed to use the Internet.

Social sites such as Facebook only permit access to people over the age of 13yrs. These sites pose a variety of dangers to young people, therefore the school endorses the restrictions. Social sites are blocked in school; parents are asked to monitor this at home. We actively discourage children from using other social media sites and children are never allowed to access them in school as they are blocked.

Any queries relating to this policy should be addressed to Miss Atkinson, Computing Subject Leader or the Head Teacher.

Yours sincerely,

Lisa Weeks	Elizabeth Atkinson
Head Teacher	Computing and E-Safety Coordinator

St James' RC Primary School
Acceptable Use Policy for Internet Access

1. School policies apply to Internet use, in particular the Safeguarding, E Safety, Computing and Equal Opportunities Policy.
2. Private use of the Internet will be agreed with the school and will be subject to the same guidelines and policies as professional use of the services being used.
3. Electronic ordering on the Internet will be in line with the financial requirements and procedures of the schools.
4. The Internet is provided for the purpose of research and communication and its use will be limited to this purpose.
5. All children in all year groups will be taught in an age appropriate way how to access the internet safely.
6. Adults competent in using the Internet will supervise **all** pupil Internet sessions.
7. Access will always be in 'public' areas where screens are visible. Internet use will be driven by clear learning intentions, which are set in the context of well framed tasks.
8. Pupils will not be given access to Newsgroups or 'chat areas.'
9. No personal details will be given out over the Internet except in carefully approved circumstances (e.g. joint projects). This will always be administrated and organised by a class teacher.
10. The school will keep its anti-virus software up to date to ensure that school activities are not disrupted by the malevolent actions of others. The implementation of this policy will be formally monitored by the school with details of upgrades being logged by the school and implemented by our ICT support provider.
11. Pupils receiving questionable materials will report these immediately to the supervising adult. All children will be taught what to do if they see something inappropriate on the internet.
12. Particular care will be taken when performing Internet searches as the search engine may accidentally return undesirable links. Teachers will always search using the same vocabulary as the children before the session to ensure that the results are appropriate.
13. All Internet users will be aware that all access is logged, and that any material accessed may subsequently be viewed by other users as well as the system administrator.
14. The school will enter into a "contract" with pupils and parents to regulate Internet use.
15. School will enter into a contract with staff to regulate the use of the Internet.
16. The school's personal computers (including portables) will only be used to access the Internet through an officially authorised route.
17. Any software downloaded from the Internet on to computers or tablets will be appropriately virus checked, licensed and registered. (Authority for this is only given to I.C.T. Subject Leader).
18. School staff will not accept pupils or past pupils of school age onto their social sites.
19. Only Year 6 are permitted to bring mobile phones to school. These must be handed in to the school office first thing in the morning and collected at the end of the day. Mobile phones that have any kind of internet capability will not be allowed on the school premises.
20. The school will manage the website with due care and attention.

St James’ RC Primary School

Acceptable Use Policy for Internet Access

Pupil and Parental Permission Form

Please read through these guidelines with the children, explaining and answering any questions they may have.

1. I will not log on to the Internet without the direct permission of a member of staff.

2. I will follow the instructions of the teacher at all times.

3. I will not send or display inappropriate messages or pictures.

4. I will not knowingly search for inappropriate material on the Internet.

5. I will not copy or down load anybody else's work from the Internet.

6. I will not use another person's password.

7. I will not open up another person's file or folder without permission from the teacher.

8. I will not print unnecessary files or pictures.

9. I will not knowingly introduce a virus onto the school system.

10. I will not contact any member of staff via any social media site.

Declaration

I have seen the rules, which apply to using the Internet and I understand that if I break any of these rules I will lose my access to the use of the Internet and further action may need to be taken.

The teaching staff check the use of the Internet and a record is kept on the school system.

Pupil’s Signature and Date: ____

As the parent or legal guardian of the pupil signing above, I grant permission for my child to access networked computer services such as electronic mail and the Internet.

I understand that some materials on the Internet may be objectionable, but I accept responsibility for my child to follow the above stated rules when selecting, sharing and exploring information and media.

Parent’s Signature and Date: _____________________________________

St James’ RC Primary School

Acceptable Use Contract for Staff

As a member of staff at St. James’ RC Primary School I agree to adhere to the Christian ethos of the school and to the high professional standards that are expected.

In respect of internet use I agree that I will act responsibly in my dealings with young people at all times. This means that:-

- I will not allow current pupils or past pupils still of school age permission to access my social sites
- I will not post pictures of pupils or of any school activity on my social site
- I will not discuss or refer to my work in school on my social site
- I will not discuss a pupil with a parent on my social site
- I will not contact pupils or past pupils of school age via any social network
- I will not post pictures of myself or colleagues in an undignified situation
- I will not use unsuitable language or make distasteful comments on my social site
- I will not photograph children in school without the permission of the Head Teacher
- I will not download pictures of pupils onto my home computer

Declaration

I have seen the rules, which apply to the private and professional use of the internet and agree to abide by them. I understand that my actions affect the safety of the pupils as well as the ethos and reputation of the school. A breach of the above rules could lead to dismissal.

Staff Signature and Date:

____