Internet Acceptable Use Policy

Name of School	**St Edward's Catholic Primary School**
Policy review date	**September 2023**
Date of next review	**September 2024**
Who reviewed this policy?	**Mrs N Middleton** **Computing Lead**

Introduction

The Internet is an environment that contains many helpful educational resources, but also many documents, images, and files that may not be suitable. This policy describes what St. Edward's Primary School deems **'acceptable use'** of technology for staff and pupils.

This policy is intended to protect school systems from any liability incurred by allowing pupils and staff access to the wealth of information on the Internet. This policy applies to all members of the school community (including staff, pupils, students on placement, governors, volunteers, parents/carers, visitors) who have access to and are users of school ICT systems, both in and out of school.

This policy will be used to deal with incidents involving pupils, in conjunction with the school's behaviour and anti-bullying policies where appropriate. The school will, where known, inform parents / carers of incidents of inappropriate Online Safety behaviour that take place out of school. For incidents involving staff, the school will refer to its disciplinary policy and procedure: any breaches of this acceptable use policy may lead to disciplinary action and, in cases of serious misconduct, may result in the employee's dismissal.

Guidelines for children

Internet and device access have been provided to equip children with the necessary resources to build on skills taught in school and at home. The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote student achievement. In order for these to be used safely, staff must encourage children to follow these guidelines:

- Children must only use computers, devices and the internet when supervised by an adult in school.
- Children must use school ICT in a responsible way to make sure that there is no risk to the safety of themselves or others. Children must follow and agree to the following guidelines:
- Children will be aware that school can monitor their use of ICT systems, email and other device use.
- Children will not share their logins or passwords for devices.
- Children will be aware of the need to create avatars and nicknames when online so as not to disclose or share their personal photograph and/or name.
- Children will be aware that they should not speak to anyone online that they do not know as this can be dangerous.
- Children will immediately report any unpleasant or inappropriate material or messages that make them feel uncomfortable.
- Children will only use school ICT devices for educational use and not for personal or recreational use unless they have permission to do so.
- Children must seek permission before accepting downloads or uploads.
- Children must not use school ICT devices for online gambling, internet shopping, video broadcasting or file sharing unless they have the permission of an adult.

- Children will respect other pupils' work and will not access, copy, edit or remove any files that do not belong to them.
- Children will only use personal "bring your own" devices (phones, USB sticks, etc.) in school with the permission of their class teacher and Headteacher. If children are using their own devices, they are to follow all the rules set out in this policy.
- Children must report any damaged devices to their class teacher who will report and log the problem using the school's website.
- Children will not use programmes or software that will enable them to bypass the Local Authority filtering systems.
- Children will not open any attachments to emails, unless they know the sender.
- When using the internet for research, children must ensure that they recognise copyright protection.
- Children must understand that ICT must be used appropriately out of school.
- Children must be aware that school may take action against them and inform their parents / carers if they are involved in incidents of inappropriate behaviour when they are out of school. Examples of this would be cyber bullying, use of images or personal information, inappropriate comments about school or other pupils on social media sites.
- Children not complying to these guidelines may risk losing the right to use ICT devices in school and staff will make parents aware of the reasons for this.

School Computer Network

- Any websites visited must comply with school restrictions. If staff or children are offended by content then this must be reported.
- Staff may not use private emails to send content that, if intercepted, would place the school in violation of laws or regulations.
- Staff may not use the internet to view illegal or seditious material that would place the member of staff or school at legal risk.
- If wanting to add or download software to be used on the school network, CompTech and the ICT coordinator must first be informed.
- Chat rooms are not to be used at any time on the school network.
- Uploading of material to the internet for use other than work related is not allowed.
- The purchasing of school related resources over the internet for school purposes should be cleared by the subject coordinator first and is subject to the same authorisation procedures and limits as purchases made by other means.
- The school network must not be used to hold or process personal data except within the provisions of the Data Protection Act 1984.
- It should be noted that authorised staff have the ability to access all user files, including email stored on central servers and data on individual computers as well as on the network.

- All staff will have read the 'PREVENT' duty guidance and will know what measures are in place when researching terrorism and counter terrorism.

Electronic Communication for Staff

At St. Edward's Primary School we take advantage from electronic communication. Emails are a permanent document and even when deleted can be retrieved from system backups. A school email address is for school use only and should therefore not be used for personal reasons. In the interest of protecting the safety of staff members, the following guidelines should be adhered to:

- When you do not know the person, remain with formal modes of address - use the form Dear Mr/Mrs, etc. and end the email with Regards, Best Wishes.
- Increasingly, parents are communicating with staff via email. When there is a need to reply and where this is preferable to a phone call, staff should CC the Headteacher and Phase Leader in to the reply. Staff should ensure they put as much thought as possible in to the reply and make sure it is grammatically accurate before sending. It might be worth asking a colleague for their opinion before hitting the SEND button.
- If the email is confidential, ensure this is marked clearly. You may want to incorporate a disclaimer as a footnote/signature such as the following:

'The information in this email is confidential and may be legally privileged. It is intended solely for the addressee(s). Access to this email by anyone else is unauthorised. If you are not the intended recipient, any disclosure, copying or distribution is prohibited and may be unlawful.'

- Do not use copyright-protected material without proper authorisation. To do so is illegal.
- When replying to an email which has been sent to other people as well, take care to reply to the author. Only select the 'Reply to all' if it is really necessary that everyone else should see your reply.
- Ensure you have an email signature. It should contain your name, title, school address and telephone number.
- Check your email regularly. If you are absent from school for a period of time, ensure you have set up an automatic reply to explain your absence.
- If you receive junk mail, delete it straight away and do not reply. If you feel it is appropriate, use the Block Sender option.
- If you receive an attachment from an unknown sender which you are not comfortable with, delete it straight away in the case of viruses and do not open or forward to others.
- If you are printing out confidential emails, ensure you collect them straight away from the printer.

- If you have enabled the facility on your Smartphone to receive and send emails, ensure your phone has a code/lock in case it gets in to the wrong hands.
- Before sending please check the recipient is who you want it to be. The sending of confidential items to the wrong recipient (and some people have the same name) is a breach of the Data Protection Act.

Social Media

For the purposes of this policy, social media includes (but is not limited to) internet forums, blogs, wikis, podcasts, photograph websites (Flickr, Animoto, etc.), Facebook and Twitter. Staff should follow these guidelines in relation to any social media sites/apps that they use, both in work and in their personal lives. These guidelines apply to all staff working at St. Edward's Primary School. This includes all teachers, teaching assistants, dinner time staff, site staff, administrative staff, governors, students on placement and volunteers. The reason for this policy is to protect the safety and integrity of staff and to assist those working with pupils to work safely and responsibly. Furthermore, it sets out to offer a code of practice relevant to social media for professional and personal use, as it is important that staff understand how to separate and differentiate between the two.

- Staff should not access social media sites from the school's computers or other school device when working in school unless it is used for educational purposes, and is previously agreed and sanctioned by the Headteacher.
- Staff should understand that anything they write (regardless of privacy settings) could be made public by other users. Staff should ensure they remain professional and ensure a clear distinction between professional and personal lives.
- Any use of social media should not:

- Bring the school in to disrepute
- Breach confidentiality
- Breach copyrights
- Bully, harass or discriminate
- Be derogatory to others or about others

- The school appreciates that people will make use of social media in a personal capacity. Staff must be aware that if they are recognised from their profile as being associated with the school then certain opinions expressed could be considered to affect the reputation of the school.
- When using social media sites, staff should not share login or password details with others.
- If using social media sites/apps on your phone ensure you have a lock/pin code to protect entry to your phone.
- Keep personal mobile and home numbers private
- Staff should restrict access on their social media sites and pages by amending privacy settings as follows:

Step 1 - Access the Privacy Settings page.
Step 2 - Under Privacy Settings and Tools, access Edit on "Who can see my stuff?"

You can manage the privacy of things you share by using the audience selector right where you post. Setting this to “Friends” means that you know who can see your posts.

- There should be no online dialogue between staff and pupils of the school.
- Staff should not make ‘friends’ of pupils at school. If a member of staff is approached by a pupil via their social media account, wishing to either ‘follow’ them or be their ‘friend’, the staff member should politely refuse or block this. Ideally, this action should then be explained to the child in school, making reference to the inappropriateness of such a connection.

Staff should also not make ‘friends’ of pupils’ parents/carers. If such an approach is made the staff member should politely refuse or block this. Ideally, this action should then be explained to the parent/carer either face to face or by telephone, making reference to the inappropriateness of such a connection and potential risks to their employment status.

- The use of Twitter for private use is extremely beneficial for CPD purposes. Personal accounts must remain so and there must be an understanding that they will reflect upon a staff member’s professionalism and therefore impact on a school’s reputation. Staff should remember that nothing should be written that they would not mind repeating in front of a colleague, parent, governor or Head teacher. The use of Twitter in school is a good way of sharing information and activities with Photographs should be taken using school devices (cameras, iPod touches, iPads).
- Photographs should not be taken or stored on personal devices (phones, iPads, laptops, etc.).

Online Safety in school

Online safety (formerly Online Safety) should be a constant focus in all areas of the curriculum and staff should reinforce Online Safety messages at all times.

- In lessons where internet use is planned, staff should endeavour to check sites beforehand to determine their suitability for use. Staff should ensure that they are vigilant in monitoring content of the websites that children visit including specifically websites that relate to radicalisation, terrorism that are a requirement of the Prevent Duty. It is accepted that at times, especially in KS2, children may need to research topics (e.g.racism, discrimination, drugs, alcohol and social media) that may result in sites being blocked.
- Staff can request that a site is temporarily accessed for the period of study time needed.
- Any request must be made with clear reasons for the need.
- Pupils should be provided with constant reminders of being critically aware of materials/content that they access online.
- Pupils should be encouraged to acknowledge sources of information used and to respect copyright when using material that has been accessed online.

- Parents/carers should be provided with guidance via the school website highlighting good practice for encouraging 'e-safe' children.

Mobile Phones

Many new mobile phones have access to the Internet and picture and video messaging.

Whilst these are the more advanced features, they present opportunities for unrestricted access to the Internet and sharing of images. There are risks of mobile bullying, or inappropriate contact.

- Pupils by permission of the Headteacher can bring mobile phones onto the school site where it is seen by the school and parents as a safety/precautionary use. These are handed in, switched off, to a secure box in their classroom when they arrive at school and are collected at the end of the day.
- The sending of abusive or inappropriate text messages is forbidden.
- Staff should always use school phone to contact parents.
- Staff including students and visitors are not permitted to access or use their mobile phones within the classroom. All staff, visitors and volunteers within the Foundation Stage place their phones in a locked cabinet in Nursery and Reception for the duration of hours worked by each member of staff. The remainder of staff ensure that their phones are turned off and stored safely away during the teaching day.
- Staff may use their mobile phones in the staffroom during the lunch period.
- Parents cannot use mobile phones on school trips to take pictures of the children

Use of digital and video images

- Digital and video images have created significant benefits to learning. Staff, pupils and parents / carers must be aware of the risks associated with sharing images and videos on the internet.
- Staff and pupils must not take, use, share, publish or distribute images of others without their permission.
- Photographs that are published on the school website or elsewhere (e.g. Twitter) should be carefully selected and should only include initials of pupils.
- Written permissions from parents / carers will be obtained as part of the admissions procedure and will be held in school. It is each staff member's responsibility to ensure that s/he checks this information and so does not publish photos or videos of these children.
- If staff are completing work for external sources for their own CPD (e.g. research projects, management courses, etc.), staff must request parental permission outlining where and why the photo or video is being used.

Parent / carer acceptable use policy

Parents are to be made aware that children must be responsible when using the internet and other communications technologies at school and at home.

- Parents / carers will be issued with a notice when their child starts at the school, which outlines the use of the internet and ICT devices in school.
- Parents / carers to be aware that their child will have had to sign an Acceptable Use Agreement in school.
- Parents / carers to understand that children will be receiving Online Safety education in school appropriate to their child's age and that staff will be following government guidance on this.
- Parents / carers will be aware that the school will take all necessary precautions to ensure that monitoring and filtering systems are in place.
- Parents / carers to understand that, although staff will take all necessary precautions, school cannot ultimately be held responsible for the nature and content of materials that may be accessed on school devices.
- Parents / carers to understand that their child's activity will be monitored and that staff will contact them should there be a deliberate breach of the Acceptable Use Policy.
- Parents / carers must be encouraged to role model safe use of the internet and devices at home and will inform school if they have concerns over their child's internet usage.
- Parents / carers taking photographs or videos at school events, e.g. concerts, sports days, etc. should not publish these on any social networking site if they contain images of any other children but their own.

Staff iPad User Agreement

- At all times any such iPad shall remain the property of the school and is subject to all of the school's standard rules, policies and procedures concerning access to, and use of, the Internet and Email. These are school devices and therefore are for professional use.
- St Edward's Primary School reserves the right to require the return of the iPad from the staff member at any time and without notice. If return of the iPad is requested, it must be handed in within 24 hours of the request being made.
- Staff issued with an iPad are expected to exercise the same care in respect of the security and upkeep of the iPad as if it were the employee's own property. In particular, it is the employee's responsibility to ensure that their allocated iPad is securely locked away at night, whether at work or at home. Similar care must be taken when leaving the iPad in a meeting room or any off-site venue and whilst travelling. iPads must not be left unattended in motor vehicles at any time.
- The iPad must always be kept and used within the case issued with it.
- The pass code for the iPad will be set up by the school before issuing the device to a member of staff. This pass code must not be changed.
- Malfunctions or any other technical problem with the iPad should be reported immediately to a member of SMT by the employee, so that steps can be taken to have the problem rectified by an approved

technician as quickly as possible. Under no circumstances is the employee to organise repairs to the iPad before reporting the problem.

- Shared use of an iPad by colleagues of the employee to whom it has been issued is permitted, provided the employee concerned is satisfied the colleague(s) in question is/are competent to use the iPad in a safe and professional manner.
- Lending the iPad to any third party is strictly prohibited. Use of an organisation-owned iPad by the employee's friends and/or family is also strictly prohibited.
- Careless loss, damage or misuse of the iPad, its case, wireless keyboard or any other associated peripheral may result in disciplinary action and, in cases of serious misconduct, may result in the employee's dismissal.
- Specific iPad Apps will be required to ensure maximum functionality of any iPad issued to an employee. Certain Apps will be mandatory and an employee issued with an iPad will be updated from time to time as to the downloading of mandatory Apps.
- Staff are able to log in with their own Apple ID and download their own Apps for use in school.

However, any Apps which would benefit other members of staff can be requested via email to either CompTech or the ICT coordinator who will be responsible for the App budget. Staff should note that the school, via its web management system, can see what Apps are installed on each iPad.
I accept all of the above points

Signed:

Name:
Date:

Make/Model: Serial No:

Staff Laptop User Agreement

- At all times any such laptop shall remain the property of the school and is subject to all of the school's standard rules, policies and procedures concerning access to, and use of, the Internet and Email. These are school devices and therefore are for professional use.
- St Edward's Primary School reserves the right to require the return of the laptop from the staff member at any time and without notice. If return of the laptop is requested, it must be handed in within 24 hours of the request being made.
- Staff issued with a laptop are expected to exercise the same care in respect of the security and upkeep of the laptop as if it were the employee's own property. In particular, it is the employee's

responsibility to ensure that their allocated laptop is securely locked away at night, whether at work or at home. Similar care must be taken when leaving the laptop in a meeting room or any off-site venue and whilst travelling. Laptops must not be left unattended in motor vehicles at any time.

- Malfunctions or any other technical problem with the laptop should be reported immediately to a member of SMT by the employee, so that steps can be taken to have the problem rectified by an approved technician as quickly as possible. Under no circumstances is the employee to organise repairs to the laptop before reporting the problem.
- Shared use of an laptop by colleagues of the employee to whom it has been issued is permitted, provided the employee concerned is satisfied the colleague(s) in question is/are competent to use the laptop in a safe and professional manner.
- Lending the laptop to any third party is strictly prohibited. Use of an organisation-owned laptop by the employee's friends and/or family is also strictly prohibited.
- Careless loss, damage or misuse of the laptop or any associated peripheral may result in disciplinary action and, in cases of serious misconduct, may result in the employee's dismissal.
- Specific software will be required to ensure maximum functionality of any laptop issued to an employee. This will be installed by the school's technician. Any other software should not be installed or downloaded without prior consultation with the school's technician and ICT co-ordinator.
- Staff may not use school laptops to view illegal or seditious material (in school or elsewhere) on the internet that would place the member of staff or school at legal risk.
-

I accept all of the above points
Signed:

Name: Date:

Make/Model: Serial No:

Any employee requiring further information about this policy should contact the Head teacher

Notice to Parents/Carers regarding Acceptable Use of ICT

At St Edward's we provide children with access to the Internet using a range of devices, such as computers, iPads, iPods, etc. The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote student achievement.

Parents / Carers should note that:

- Children must be responsible when using the internet and other communications technologies at school and at home.
- Children use devices and the internet in school.

- Children receive Online Safety education in school appropriate to their age; staff follow government guidance on this.
- School will take all necessary precautions to ensure that monitoring and filtering systems are in place. However, school cannot be ultimately responsible for the nature and content of materials that may be accessed.
- Children's activity will be monitored and a member of staff will contact me should there be a deliberate breach of the school's Acceptable Use Policy.
- They should ensure that they role model safe use of the internet on devices at home and inform school if they have concerns over their child(ren)'s internet usage.
- Children sign an Acceptable Use Agreement in school.
- The legal minimum age for having a Facebook account is 13. This is similar to other social media accounts as children below this age are not always aware of the impact of their messages.
- Any photographs or videos that parents/carers take at school events, e.g. concerts, sports days, etc. should not be published on any social networking site if they contain images of any other children but their own.
- Unless we are notified by parents/carers to the contrary, we will assume that they are happy with their child(ren)'s use of the internet and devices within school.

Think before you click

S 	**I will only use the Internet and email with an adult present.**
A 	**I will only click on icons and links when I know they are safe**
F 	**I will only send friendly and polite messages**
E 	**If I see something I don't like on a screen, I will always tell an adult**

My Name:

My Signature:

KS2 Pupil Acceptable Use Agreement

These rules will keep me safe and help me to be fair to others.

- I will only use the school's computers for schoolwork and homework.
- I will only edit or delete my own files and not look at, or change, other people's files without their permission.
- I will keep my logins and passwords secret.
- I will not bring files into school without permission or upload inappropriate material to my workspace.
- I am aware that some websites and social networks have age restrictions and I should respect this.
- I will not attempt to visit Internet sites that I know to be banned by the school.
- I will only e-mail people I know, or a responsible adult has approved.
- The messages I send, or information I upload, will always be polite and sensible.
- I will not open an attachment, or download a file, unless I know and trust the person who has sent it.
- I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless a trusted adult has given permission. I will never arrange to meet someone I have only ever previously met on the Internet, unless my parent/carer has given me permission and I take a responsible adult with me.
- If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will show a teacher / responsible adult.

I have read and understand these rules and agree to them.

School logo	Name of School	St Edward's
	AUP review Date	2023
	Date of next Review	2024
	Who reviewed this AUP?	

Signed: *Date:*

Acceptable Use Policy (AUP): Staff agreement form

This policy covers use of digital technologies in school: i.e. email, Internet, intranet and network resources, learning platform, software, equipment and systems.

- I will only use the school's digital technology resources and systems for Professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.
- I will not reveal my password(s) to anyone.
- I will follow 'good practice' advice in the creation and use of my password. If my password is compromised, I will ensure I change it. I will not use anyone else's password if they reveal it to me and will advise them to change it.
- I will not allow unauthorised individuals to access email / Internet / intranet / network, or other school / LA systems.
- I will ensure all documents, data etc., are saved, accessed and deleted in accordance with the school's network and data security and confidentiality protocols.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will only use the approved, secure email system(s) for any school business.
- I will only use the approved school email, school Learning Platform or other school approved communication systems with pupils or parents/carers, and only communicate with them on appropriate school business.
- I will not browse, download or send material that could be considered offensive to colleagues.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the appropriate line manager / school named contact.
- I will not download any software or resources from the Internet that can compromise the network, or are not adequately licensed.
- I will not publish or distribute work that is protected by copyright.
- I will not connect a computer, laptop or other device (including USB flash drive), to the network / Internet that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the school's recommended anti-virus, firewall and other ICT 'defence' systems.
- I will not use personal digital cameras or camera phones for taking and transferring images of pupils or staff without permission and will not store images at home without permission.
- I will use the school's Learning Platform in accordance with school protocols.
- I will ensure that any private social networking sites / blogs etc that I create or actively contribute to are not confused with my professional role.

- I agree and accept that any computer or laptop loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- I will access school resources remotely (such as from home) only through the LGfL / school approved methods and follow e-security protocols to access and interact with those materials.
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.
- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I will embed the school's Online Safety curriculum into my teaching.
- I will alert the school's named child protection officer / relevant senior member of staff if I feel the behaviour of any child I teach may be a cause for concern.
- I will only use LA systems in accordance with any corporate policies.
- I understand that all Internet usage / and network usage can be logged and this information could be made available to my manager on request.
- I understand that it is my duty to support a whole-school safeguarding approach and will report any behaviour (of other staff or pupils), which I believe may be inappropriate or concerning in any way, to a senior member of staff / named child protection officer at the school.
- I understand that failure to comply with this agreement could lead to disciplinary action.

Acceptable Use Policy (AUP): Staff agreement form

User Signature

I agree to abide by all the points above. I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent Online Safety policies. I wish to have an email account; be connected to the Intranet & Internet; be able to use the school's ICT resources and systems.

Signature ..... Date .....

Full Name ..... (printed)

Job title .....

Authorised Signature (Head Teacher)

I approve this user to be set-up.

Signature ..... Date.....

Full Name ..... (printed)