William Cassidi Church of England Primary School

Internet Usage Policy Statement

'Life in all Fullness'
(John 10:10)

As a school, we want to provide children with the very best education. To let them experience life in all its fullness and living with all their heart. Our main core value of love underpins all that we do. Our school is Christ-centred and our core Christian values of love, respect, courage, service and resilience flow through every aspect of school life. It is on this bedrock that we provide an excellent education for the children who attend our school. We want every child to be the very best that they can be and to recognise that they are precious, loved and valued.

Policy Aim

Our school's Internet Acceptable Use Policy runs alongside and compliments our e-Safety Policy and will relate to other policies including those for behaviour and for personal, social and health education, including citizenship. This Internet Acceptable Use Policy has been devised by a team consisting of the Headteacher, ICT Co-ordinator and pupils and will be reviewed on a yearly basis. It has been agreed by the Senior Leadership Team and has been discussed and approved by Governors. This document is based upon good practice set out by The National Grid for Learning (NgfL), UK Council for Child Internet Safety and the Northern Grid for Learning's AUP Policy.

Policy approved by the Governing Body: December 2024
To be reviewed: December 2025

Written by Mr M Proud (Internet Rules in cohesion with E-Safety Ambassadors)

The Importance of the Internet in Learning in Schools:

The purpose of Internet access in school is to raise educational standards, to support the professional work of staff and to enhance the school's management information and business administration systems. Access to the Internet is a necessary tool for staff and pupils. It is an entitlement for everyone but all must use it in a responsible manner. If anyone does not follow the Internet rules appropriate consequences will be imposed.

How the Use of the Internet Benefits the School:

A number of studies and government projects have indicated the benefits to be gained through the appropriate use of the Internet in education.
These benefits include:

- Access to world-wide educational resources including museums and art galleries
- Inclusion in government initiatives such as NGfL and the Virtual Teacher Centre
- Information and cultural exchanges between pupils world-wide
- Cultural, social and leisure use in libraries, youth clubs and at home
- Discussion with experts in many fields for pupils and staff
- Staff professional development - access to educational materials and good curriculum practice.
- Communication with the advisory and support services, professional associations and colleagues
- Improved access to technical support
- Exchange of curriculum and administration data with the Stockton LA and DfE.

Using the Internet to Provide Effective Learning:

Teachers, parents and pupils need to develop good practice in using the Internet as a tool for teaching and learning. There is a fine balance between encouraging autonomous learning and maintaining adequate supervision. Systems that ensure Internet use is as

safe as possible will enable increased use and the quality of that use is a critical factor. Internet access is provided by BT. This is controlled and maintained by One IT with whom the school has a Service Level Agreement. One IT provides a service designed for pupils which includes filtering system (currently Smoothwall) that is appropriate to the age of the pupils at William Cassidi School.

- Internet access will be planned to enrich and extend learning activities
- Access levels will be reviewed to reflect the curriculum requirement
- Pupils will be given clear objectives for Internet use
- Staff will select sites that will support the learning outcomes planned for pupils' age and maturity
- Pupils will be educated in taking responsibility for Internet access
- Children will be encouraged to use a Virtual Learning Environment for personal development (The E-schools learning Platform).

How Pupils Will Be Taught to Assess Internet Content:

Pupils in school are unlikely to see inappropriate content in books due to selection by publishers and teachers. This level of control is not so straightforward with Internet-based materials. Therefore, teaching should be widened to incorporate Internet content issues, for instance the value and credibility of Web materials in relationship to other media.

- Pupils will be taught ways to validate information before accepting that it is necessarily true
- Pupils will be taught to acknowledge the source of information and observe copyright when using Internet material for their own use
- Pupils will be made aware that the writer of an e-mail or the author of a Web page might not be the person claimed
- Pupils will be encouraged to tell a teacher/responsible adult or the ICT Co-Ordinator (Mr Proud) if they encounter any material that makes them feel uncomfortable.

Online Relationships

- That people sometimes behave differently online, including by pretending to be someone they are not;
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous;
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them;
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met.
- How information and data is shared and used online.

The Management of E-mail/Messaging:

E-mail/Messaging is an essential means of communication within education. The school provides email accounts for all staff and some Year 6 pupils. Y2 – Y6 pupils have instant messaging capability.

- Pupils need to use e-mail/messaging as part of their development in Computing/ICT
- Pupils may send e-mail/a message as part of planned lessons or a message as their involvement of the E-Learning Platform. This assumes a high level of trust and pupils will be asked to sign the Acceptable Use Statement
- In coming e-mail/messages will be regarded as public
- Received e-mail/messages may be examined
- The forwarding of chain letters will be banned, as will the use of chat lines.

The Management of the School's Website:

At William Cassidi it is our intention that our website showcases our school and provides a hub of information for parents/carers and prospective parents/carers. It provides useful information about the school, its ethos, important events and dates. Ground rules are important to ensure that the website reflects the school's ethos and that information is accurate and well presented. As the school's website can be accessed by anyone on the Internet, the security of staff and pupils must be considered carefully:

- The Headteacher will delegate editorial responsibility to a member of staff to ensure that content is accurate and quality of presentation is maintained
- The point of contact on the website should be the school address and telephone number. Home information or individual e-mail identities will not be published
- The school's current policy regarding Data Protection (GDPR) will be adhered to at all times
- Written permission from parents will be sought annually before photographs of pupils are published on the school website.

The Availability of Other Internet Applications:

The Internet is the underlying technology, but new applications are being developed to use this ability to communicate, such as Chat, Newsgroups and webcams. Many of these facilities have great potential for education, for instance pupils exchanging live text, speech or video with a similar class in another location around the country or world, at low cost. However, most new applications start without the needs of young users being considered, particularly the area of security:

- Pupils will not be allowed to access public chat rooms or social media platforms
- Newsgroups are only available to staff
- New facilities will be thoroughly tested before pupils are given access.

The Authorisation of Internet Access:

In school, all staff and all pupils will be granted access to the Internet as a blanket requirement, with a single written record made by the Headteacher to this effect. Parental permission will be required before children can access the Internet and e-mail:

- Internet access is a necessary part of statutory curriculum. It is an entitlement for pupils, which is based upon responsible use
- In the Foundation Stage and Key Stage I, the majority of the access to the Internet will be by teacher or adult demonstration. However, there may be situations when children have supervised access to specific approved on-line materials
- In Key Stage 2, Internet access will be granted to a whole class as part of the scheme of work, after a suitable education in the responsible use of the Internet
- Parents will be informed that pupils will be provided with supervised Internet access
- Parents will be asked to sign and return a permission form
- Pupils must also, along with parents/carers, sign the letter sent home. This will be an indication by the parents and pupils that they have discussed understand and accept the implications of the use the Internet in school and at home
- A record will be maintained of all staff and pupils, on a whole class basis, with Internet access.

The Assessment of Risk When Using the Internet in School:

It is difficult to completely remove the risk that pupils might access unsuitable materials via the school system. In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will supervise pupils and take all reasonable precautions to ensure that user's access only appropriate material, including the use of its current filtering software. However, due to the international scale and linked nature of information available via the Internet, it is not possible to guarantee that unsuitable material will never appear on a terminal. Neither the school nor Stockton L.A. can accept liability for the material accessed, or any consequences thereof.

Ensuring Safe Internet Access:

Access to appropriate information should be encouraged but Internet access must be safe for all members of the school community from the youngest pupil to the teacher and administrative staff. The Internet is a communications medium that is freely available to any person wishing to send e-mail or publish a website on almost any topic. Pupils will generally need protected access to the Internet. Children will be given protected access to the Internet.

The technical strategies used by the school to restrict access to inappropriate material fall into several overlapping types (sometimes all referred to as filtering) are as follows:

Blocking strategies: Removing access to a list of unsuitable sites or newsgroups. Maintenance of the blocking list is a major task, as new sites appear every day.

Filtering: Examining the content of web pages or e-mail messages for unsuitable words. Blocking and filtering, as previously stated, is performed by One IT on the school's behalf:

- Pupils will be informed that Internet use will be supervised and monitored
- The school will work in partnership with OneIT to ensure systems to protect pupils are constantly reviewed and improved where appropriate
- The ICT Co-Ordinator will make sure that occasional checks are made to ensure that the filtering methods selected are effective in practice
- If staff or pupils discover unsuitable sites, the URL (address) and content will be reported to the school's designated ICT Technician from One IT, via the ICT Co-ordinator, which will promptly block such sites
- Any material that the school suspects is illegal will be referred to the ICT Co-ordinator who will report this to the Senior Leadership Team

The Maintenance of Security of the ICT Systems:

The Internet is a connection to the outside world that could compromise system performance or threaten security.

- Security strategies will be discussed with One IT
- One IT is regularly reviewing the schools' networks to ensure that the system has the capacity to take increased traffic caused by Internet use
- The security of the whole system will be reviewed with regard to threats to security from Internet access.
- Personal data (e.g. photos) should not be sent over the Internet from unless the E-schools' Learning Platform is used and then only with parent consent as per school policy)
- Virus protection will be installed and updated regularly
- An individual virus scan check will be carried out once a fortnight on all machines within the ICT Suite
- Staff will check all data-sticks for viruses when attaching to the computer if used. No data-sticks will be used to transport data relating to children or other sensitive information. Staff will Use 'direct access and a laptop has been provided to each member of the teaching staff to facilitate this.
- If visitors wish to use a data-stick this will be scanned prior to use.

The Complaints Procedure Regarding Internet Use:

Prompt action will be required if a complaint is made. The facts of the case will need to be established, for instance whether the issue has arisen through Internet use inside or outside school. Transgressions of the rules could include minor as well as the potentially serious consequences and a range of sanctions will be devised, linked to the school's behaviour and e-Safety policy:

- Responsibility for handling incidents will be given to the ICT Co-ordinator and Headteacher
- Pupils and parents will be informed of the complaints procedures
- Parents and pupils will need to work in partnership with staff to resolve issues
- There may be occasions when the police must be contacted. Early contact will be made to establish the legal position and discuss strategies

- Sanctions available include interview/counselling by Head Teacher or ICT Co-ordinator and, if appropriate, informing parents or carers
- A pupil may have e-mail, Internet or computer access denied for a period of time depending on the nature of the incident
- Denial of access could include all school work held on the system
- If there is reasonable doubt of proper use the ICT Coordinator may access any persons account in order to establish whether use is appropriate or not.

Staff and Pupil Consultation about the Internet:

It is very important that staff feel prepared for Internet use and consider that the school Internet Acceptable Use Policy is appropriate. Staff should be given opportunities to discuss the issues and develop appropriate teaching strategies. It would be unreasonable if staff, particularly supply staff, were asked to take charge of an Internet activity without training. Reassurance and discussion may be required:

- Rules for Internet access will be posted near computer systems. **The Acceptable Use Statement** or **Rules for Responsible Internet Use** will be printed as posters
- All staff including teachers, supply staff, Teaching Assistants and support staff, will be provided with the Internet Access Policy, and its importance explained
- Parents' attention will be drawn to the Policy in newsletters, the school brochure, on the school Website and Eschools class page
- A module on responsible Internet use will be included in the PSHE curriculum covering both school and home use
- All new pupils to the school have an 'ICT Induction' upon starting with the school. This includes guidance on the rules of the school regarding the use of computers/Internet and how to keep themselves safe. At that time their individual access and passwords will be generated.

Enlisting Parental Support for the Use of the Internet:

Internet use in pupils' homes is commonplace. Unless parents are aware of the dangers, pupils may have unrestricted access to the Internet and as such the school would willingly help parents plan appropriate, supervised use of the Internet at home:

- A careful balance between informing and alarming parents will be maintained
- Demonstrations and practical ICT sessions for parents may be organised to encourage a partnership approach
- Joint home/school guidelines on issues such as safe Internet use will be established
- Suitable educational and leisure activities that make responsible use of the Internet will be developed with parents
- A stock of relevant leaflets from organisations such as CEOP will be maintained.

Appendix 1:

Staff ICT Acceptable Use Policy 2024/2025

As a professional organisation with responsibility for children's safeguarding it is important that all staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. All members of staff have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. To ensure that members of staff are fully aware of their professional responsibilities when using Information Communication Technology and the school systems, they are asked to read and sign this Acceptable Use Policy.

This is not an exhaustive list and all members of staff are reminded that ICT use should be consistent with the school ethos, other appropriate policies and the Law.

- I understand that Information Systems and ICT include networks, data and data storage, online and offline communication technologies and access devices. Examples include mobile phones, digital cameras, email and social media sites.
- School owned information systems must be used appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.
- I understand that any hardware and software provided by my workplace for staff use can only be used by members of staff and only for educational use. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate.
- I will respect system security and I will not disclose any password or security information. I will use a 'strong' password (A strong password has numbers, letters and symbols, with 8 or more characters, does not contain a dictionary word and is only used on one system).
- I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the ICT Co-ordinator.
- I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the Data Protection Act 2018, General Data Protection Regulation May 2018, School Policy and any update of these. This means that all personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online (only within sites with suitable data protection controls) or accessed remotely. No data will be removed from the school site on memory sticks and I understand that I will access any such data via the 'direct access' method provided. Any images or videos of pupils will only be used in a manner approved by parents/carers and stated within the appropriate school's policy.
- I will not keep professional documents which contain school-related sensitive or personal information (including images, files, videos etc.) on any personal devices. I will use the School Direct Access, remote access and E-Learning Platform to

upload any work documents and files in a password protected environment. I will protect the devices in my care from unapproved access or theft.

- I will respect copyright and intellectual property rights.
- I have read and understood the school E-Safety policy which covers the requirements for safe ICT use, including using appropriate devices and the safe use of social media websites.
- I will report all incidents of concern regarding children's online safety to the Designated Child Protection Officer (Mrs. J. Campbell) and the E-Safety Co-ordinator (Mr. Proud) as soon as possible.
- I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to the E-Safety Co-ordinator.
- I will not attempt to bypass any filtering and/or security systems put in place by the school. If I suspect a computer or system has been damaged or affected by a virus or other malware or if I have lost any school related documents or files, then I will report this to the ICT Co-ordinator (Mr. Proud) as soon as possible.
- I will promote e-Safety with the pupils in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.
- If I have any queries or questions regarding safe and professional practise online either in school or off site, then I will raise them with the e-Safety Co-ordinator or the Headteacher.

Use of Social Media Sites:

Introduction:

The Governing Body of William Cassidi C of E Primary School is committed to ensuring that all staff are aware of their responsibilities in connection with the use of the Internet and social media applications that allow users to interact with one another. Examples of such sites include, but are not limited to, blogs (short for web log), Facebook, Instagram, WhatsApp, X, Bebo, YouTube, Windows Live Spaces, Snapchat, forums, bulletin boards, multiplayer online gaming, chatrooms, Wikipedia and instant messenger.

While acknowledging the benefits of these applications for opportunities for communication it is recognised that the Internet is a fast moving technology and it is impossible to cover all circumstances or emerging media, however the principles set out in this policy must be followed irrespective of the medium. Staff are expected to keep a professional distance from pupils and there should be a clear separation of the private social lives of staff and that of pupils.

It is important that staff are able to use technology services effectively and flexibly whilst ensuring that they do not make themselves vulnerable. However, it is also important to ensure that this is balanced with the Governing Body's duty to safeguard children/staff, the reputation of the school, the wider community, the Local Authority and the Diocese.

For staff members own security all communication via social media sites should be made with the awareness that anything said, shown or received could be made available, intentionally or otherwise, to an audience wider than that

originally intended. It is therefore advised that staff members follow the following procedures:

I. Staff members must not access social media sites for personal use via school information systems or using school equipment;
II. Care should be taken to avoid using language which could be deemed as offensive to others and be accurate, fair and transparent when creating or altering online sources of information on behalf of the School;
III. Staff members must not identify themselves as employees of the School or the Local Authority in their personal webspace. This is to prevent information on these sites from being linked with the School, the Local Authority and the Diocese and to safeguard the privacy of staff members, particularly those involved in providing sensitive frontline services. 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.
IV. Staff members must not accept pupils or ex pupils under the age of 16 years along with their parents/guardians as friends – personal communication could be considered inappropriate and unprofessional and makes staff very vulnerable to allegations;
V. Staff members should not place inappropriate photographs or post indecent remarks on any social network space;
VI. If a member of staff receives messages on his/her social networking profile that they think could be from a pupil or their parents/guardians they must report it to their Head teacher promptly and contact the internet service or social networking provider so that they can investigate and take the appropriate action;
VII. Staff members are advised not to write about their work but where a member of staff chooses to do so, he/she should make it clear that the views expressed are his/hers only and do not reflect the views of the school/Local Authority. However, all other guidelines in this policy must be adhered to when making any reference to the workplace;
VIII. Staff members must not disclose any information that is confidential to the school or disclose personal data or information about any individual/colleague/pupil, which could be in breach of the General Data Protection Regulations (GDPR 2018);
IX. Staff must not disclose any information about the school/Local Authority that is not yet in the public arena or relates to their employment at the school
X. In no circumstances should staff post photographs of pupils;
XI. Staff should not make defamatory remarks about the school/colleagues/pupils/the Local Authority or the Diocese or post anything that could potentially bring the school/Local Authority/ Diocese into disrepute;
XII. Staff members 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;

XIII. The school does not expect staff members to discontinue contact with their family members via personal social media once the School starts providing services for them. However, any information staff members obtain in the course of their employment must not be used for personal gain nor be passed on to others who may use it in such a way;

XIV. On leaving the school service, staff members must not contact school pupils by means of personal social media sites. Similarly, staff members must not contact pupils from their former schools by means of personal social media;

XV. Staff members are strongly advised to ensure 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.

Breaches of the Policy:

- The Governing Body does not discourage staff from using social media sites. However, all staff should be aware that the Governing Body will take seriously any occasions where the services are used inappropriately. If occasions arise that could be deemed to be online bullying or harassment, these will be dealt with in line with the appropriate procedures.
- A breach of this policy leading to breaches of confidentiality, or defamation/damage to the reputation of the School/Local Authority/Diocese or any illegal acts or acts that render the school/Local Authority/ Diocese liable to third parties may result in disciplinary action. Depending on the seriousness of the allegations, the disciplinary action may lead to dismissal.
- There may be instances where the school/Local Authority or Diocese will be obliged to inform the police of any activity or behaviour for which there are concerns as to its legality.

I understand that my use of the information systems, Internet and email may be monitored and recorded to ensure policy compliance. The School may exercise its right to monitor the use of information systems, including Internet access and the interception of e-mails in order to monitor compliance with this Acceptable Use Policy and the School's Data Security Policy.

Where it believes unauthorised and/or inappropriate use of the service's information system or unacceptable or inappropriate behaviour may be taking place, the School will invoke its disciplinary procedure. If the School suspects that the system may be being used for criminal purposes or for storing unlawful text, imagery or sound, the matter will be brought to the attention of the relevant law enforcement organisation.

I have read and understood and agree to comply with the Staff ICT Acceptable Use Policy.

Signed: ..... Print Name: ..... Date: .....

Appendix 2:

William Cassidi C of E Aided Primary School

Rules for Responsible Internet Use
KS2 pupils

The school has installed computers and Internet access to help my learning.
These rules will keep everyone safe and help me to be fair to others.

I promise – to only use the school ICT for schoolwork that the teacher has asked me to do.
I promise – not to look for or show other people things that may be upsetting.
I promise – to show respect for the work that other people have done.

I will not – use other people's work or pictures without permission to do so.
I will not – damage the ICT equipment, if I accidentally damage something I will tell Mr Proud or my teacher.
I will not – share my password with anybody. If I forget my password I will let Mr Proud know.
I will not – use other people's usernames or passwords.
I will not – share personal information online with anyone.
I will not – download anything from the Internet unless my teacher has asked me to.
I will – let Mr Proud or my teacher know if anybody asks me for personal information.
I will – let Mr Proud or my teacher know if anybody says or does anything to me that is hurtful or upsets me.
I will – be respectful to everybody online; I will treat everybody the way that I want to be treated.
I understand – that some people on the Internet are not who they say they are, and some people can be nasty. I will tell Mr Proud or my teacher if I am ever concerned in school, or my parents if I am at home.
I understand – if I break the rules in this charter there will be consequences of my actions and my parents will be told.

Signed (Student):

Date:

Appendix 3:

William Cassidi C of E Aided Primary School

Rules for Responsible Internet Use
KS1 pupils

The school has installed computers and Internet access to help my learning.

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

We tell our teacher or Mr Proud if anything on the computer makes us sad or worried.

I will listen carefully to instructions when in the ICT Suite.

I will be polite and behave well on the computer.

I will only use the computer when my teacher tells me to and there is an adult present.

I will use the programme or website that my teacher wants me to.

Appendix 4:

Dear Parents

Responsible Use of the Internet:
As part of pupils' curriculum enhancement and the development of ICT skills, William Cassidi C of E Primary School is providing supervised access to the Internet including the e-Schools Learning Platform and messaging. A Data-Sharing Agreement is in place between school and e-Schools outlining the acceptable use of personal data within this service.

Although there have been concerns about pupils having access to undesirable materials, we are taking positive steps to deal with this risk in school. Our school has a service Agreement with One IT, which charges them to provide a child appropriate filtering system to restrict all access to inappropriate materials.

Whilst every endeavour is made to ensure that suitable restrictions are placed on the ability of children to access inappropriate materials, the School cannot be held responsible for the nature or content of materials accessed through the Internet.

The School will not be liable under any circumstances for any damages arising from your child's use of the Internet facilities.

I enclose a copy of the Rules for Responsible Internet Use that we operate at William Cassidi C of E Primary School. We would ask that you discuss all rules with your child/children. All KS2 children are asked to read, discuss and then sign their rules themselves. KSI children are not asked to sign but are made aware of the rules at regular intervals within school. We also have a number of leaflets from national bodies that explain issues further and also cover Internet use at home.

Should you wish to discuss any aspect of Internet Use please telephone me to arrange an appointment.

Yours sincerely,

Mrs J Campbell
Head Teacher

Permission for Internet Access:

Parent/Carer's permission.

I give permission for (child/children's names) ..... to access to the Internet within school on the terms set out in the above letter.

Signed :
Print name: Date: