St Chad's RC Primary School

E-Safety and Acceptable Use of IT Policy

(January 2021)

Introductory Statement

Technology provides instant access to a wealth of up-to-the minute information and resources from across the world. Use of email, mobile phones and internet messaging applications all enable improved communication and facilitate the sharing of data and resources.

However, the dangers associated with the internet and technology means that it is paramount that we safeguard both pupils and staff at school. Some of the risks which we must seek to reduce include:

- **Children and staff inadvertently accessing content of an unsavoury, distressing or offensive nature on the internet or receiving inappropriate or distasteful materials.**

- **Children and staff receiving unwanted or inappropriate communications from known or unknown senders, or being exposed to abuse, harassment or 'cyber-bullying' via email, text or instant messaging, in chat rooms or on social-networking websites.**

We believe that, when balanced, the social and educational benefits which are gained by using electronic media mean that the advantages far out-weigh the risks, so long as users are made aware of the issues and concerns and receive ongoing education in choosing and adopting safe practice and behaviour.

Access to these electronic media help ensure:

- **Children and/or young adults are equipped with skills for the future.**
- **Instant access to a wealth of up-to-date information and resources from across the world.**
- **That children's reading and research skills are improved.**
- **That good social and communication skills are fostered and developed.**

Online learning and internet safety

St. Chad's aims to offer a safe online environment through filtered internet access. We recognise the importance of teaching pupils about online safety and their responsibilities when using communication technology.

We will ensure that the use of filtering and monitoring does not cause "over blocking" which may lead to unreasonable restrictions as to what pupils can be taught.

St. Chad's puts comprehensive filtering systems in place to prevent children accessing terrorist and extremist material, in accordance with the school's Prevent duty.

At the start of each school year pupils will be taught about the potential dangers on the internet and about e-safety as part of the Computing curriculum and whole school assemblies.

Pupils caught misusing or attempting to misuse technology and the internet will be reported to the headteacher.

The ICT technician will keep the internet filters up-to-date, to avoid misuse.

Health and safety

All electrical wires and sockets, where possible, are kept out of the way of the pupils.

Faulty electrical or damaged electrical equipment must be reported to the ICT technician or site manager to be checked and assessed to establish if it is safe to use.

Pupils will be given a five minute break if they're using the computer for more than two hours at a time.

Authorised use of facilities

IT facilities should only be used to complete school-related work. This includes, but is not be limited to:

- Preparing work for lessons, meetings, activities, reviews, etc.
- Researching for any school related task.
- Undertaking school-encouraged tuition, CPD, or for other educational benefit.
- Collating or processing information for school business.

Personal email accounts are only permitted if they have anti-virus protection approved by the ICT technician. Access to personal emails must not interfere with work duties.

Authorised use of communications facilities

The communication facilities provided by St. Chad's should only be used as required by school-related duties. Authorised use of the communications facilities includes, but is not be limited to:

- Preparing work for lessons, meetings, activities, reviews, etc.
- Researching for any school-related task.
- Any school-encouraged tuition or educational use.

Unauthorised use of facilities

It is not permitted under any circumstance to:

- Use IT facilities for commercial or financial gain, unless authorised in writing by the headteacher.
- Physically damage the IT facilities.
- Relocate, remove from the school, or otherwise interfere with IT facilities without the authorisation of the ICT technician or headteacher. Certain items are asset registered and security marked; their location is recorded by the School Business Manager for accountability. Once items are moved after authorisation, staff are responsible for notifying the School Business Manager of the new location. The exception to this is when items are moved to a secure room for insurance purposes over holiday periods.

- **Use or attempt to use someone else's user account. All users of the IT facilities will be issued with a unique user account and password. This password must be changed at regular intervals. User passwords must never be disclosed to or by anyone.**

It is not permitted to use the IT facilities at any time to access, download, send, receive, view or display any of the following:

- **Any material that is illegal**
- **Any message that could constitute bullying, harassment (including on the grounds of sex, race, religion/religious belief, sexual orientation or disability) or any negative comment about other persons or organisations**
- **Remarks relating to a person's sexual orientation, gender assignment, religion, disability, age, race or ethnicity**
- **Online gambling**
- **Remarks, which may adversely affect the reputation of any organisation or person, whether or not users know them to be true or false**
- **Any sexually explicit content**
- **Generate messages or documents that appear to originate from someone else, or otherwise impersonate someone else.**

All users must not:

- **Install hardware or software without the consent of the ICT technician or the headteacher.**
- **Introduce any form of stand-alone software or removable hardware likely to cause malfunctioning of the IT facilities or that will bypass, over-ride or overwrite the security parameters on the network or any of the school's computers. This is illegal under the Computer Misuse Act 1998.**
- **Use or attempt to use the school's IT facilities to undertake any form of piracy, including the infringement of software licenses or other copyright provisions whether knowingly or not – this is illegal.**
- **Purchase any IT facilities without the consent of the ICT technician or headteacher. This is in addition to any purchasing arrangements followed according to school policy.**
- **Use or attempt to use the school's phone lines for internet or email access unless given authorisation by the headteacher. This includes using or attempting to use any other form of hardware capable of telecommunication, regardless of ownership.**
- **Use any chat-lines, bulletin boards or pay-to-view sites on the internet.**
- **Use the internet for any auctioning activity or to purchase items, unless given authority to do so by the headteacher**
- **Knowingly distribute or introduce a virus or harmful code onto the school's network or computers. Doing so may result in disciplinary action, including summary dismissal.**
- **Use the IT facilities for personal use without the authorisation of the headteacher. This authorisation must be requested on each occasion of personal use.**

- Copy, download or distribute any material from the internet or email that may be illegal. This can include computer software, music, text, and video clips. If it is not clear that permission has been granted, or if the permission cannot be obtained, do not do so.
- Obtain and post on the internet, or send via email, any confidential information about other employees, the school, parents of pupils or suppliers.
- Interfere with someone else's use of the IT facilities.
- Be wasteful of resources, particularly printer ink, toner and paper.
- Use the IT facilities when it will interfere with responsibilities to supervise pupils.
- Use email or the internet for unauthorised purposes, this is likely to result in disciplinary action including summary dismissal.

Responsibilities

Overall responsibility for monitoring the teaching of Computing and use of technology throughout the school lies with senior management.

Senior management will make decisions on:

- How technology should support, enrich and extend the curriculum.
- The provision and allocation of resources.
- The ways in which developments can be assessed, and records maintained.
- How technology can benefit the aims and objectives of the school.

Senior management will also be responsible for overseeing the review of this IT Policy with the subject leader.

The subject leader will be responsible for monitoring the progression of teaching and learning. The subject leader is also responsible for:

- The implementation of the IT Policy across the school.
- Maintaining resources and advising staff on the use of materials.
- Assisting senior management in deciding on the allocation of resources.
- Supporting teaching staff, advising and offering to share their expertise and experience.
- Leading staff training on new initiatives.
- Monitoring the quality and progression of teaching and learning.
- Helping staff in planning future lessons and assessments.

Classroom teachers will be expected to:

- Plan and deliver interesting and engaging lessons that adhere to the national curriculum.
- Provide equality of opportunity through their teaching approaches and methods.
- Keep up-to-date assessment records.

- **Ensure pupils' development of skills and knowledge progresses through their learning and understanding of Computing.**
- **Set pupils suitable targets based on prior attainment.**
- **Maintain an enthusiastic approach to IT.**
- **Skilfully use technology across the curriculum where appropriate**
- **Promote e-safety whenever the children use technology**

An ICT technician will available to maintain and keep equipment in good running order.

The ICT technician will visit the school once a week and any issues or broken equipment will be reported to them, the technician will also be responsible for:

- **Adjusting access rights and security privileges in the interest of the school's data, information, network and computers.**
- **Carrying out checks on all computers when required.**
- **Disabling user accounts of staff that do not follow the policy and Acceptable Use Agreement, at the request of the headteacher.**
- **Assisting staff with authorised use of the IT facilities, if required.**
- **Assisting the headteacher in all matters requiring reconfiguration of security and access rights, and in all matters relating to the IT Policy.**
- **Monitor the computer logs on the school's network and report inappropriate use to the headteacher.**
- **Accessing files and data to solve problems for a user, with their authorisation – if an investigation is required by the headteacher, authorisation from the user is not required.**

Parents will be asked to support the implementation of the Computing curriculum by encouraging their child's use of the computer at home. Parents will be made aware of e-safety and will be encouraged to promote this at home.

When administering tasks to be completed at home or remote learning, teachers will be sensitive to the fact pupils may not have access to a computer at home.

Procedures for Use of our Shared Network

This section outlines what users must and must not do when using a PC / laptop connected to a network:

- **Staff must only access the network using their own passwords. These must not be disclosed or shared.**
- **Visitors (eg- supply staff) wishing to access the network must first read and agree to abide by this e-safety policy.**
- **Users must respect confidentiality and attempts should not be made to access another individual's personal folder on the network without permission.**
- **Software must not be installed without prior permission from the person responsible for managing the network.**
- **Machines must never be left 'logged on' and unattended. If a machine is to be left for a short while, it must be 'locked.'**
- **Machines must be 'logged off' and shut down correctly after use.**

Procedures for Use of the Internet and Email

This section outlines the procedures for safe internet and email at our school:

- **All pupils and staff must sign an Acceptable Use Agreement before access to the internet and email is permitted in the establishment.**
- **Users must access accounts which use app or the internet using their own username/ password and not those of another individual. Passwords must remain confidential and no attempt should be made to access another user's account.**
- **Children must be supervised at all times when using the internet or email.**
- **Procedures for safe internet use and sanctions applicable if rules are broken will be discussed with all children on an annual basis.**
- **Accidental access to inappropriate, abusive or racist material is to be reported without delay to the Headteacher, ICT Coordinator or ICT Technician and a note of the offending website address (URL) taken so that it can be blocked.**
- **Internet and email filtering software is installed to restrict access, as far as possible, to inappropriate or offensive content and to reduce the receipt of 'spam,' junk, malware or unwanted correspondence. This is to be reviewed and updated regularly.**
- **Any usernames or passwords to be used on online platforms assigned to individual pupils will not be in a form which makes them easily identifiable to others.**
- **Users must not disclose any information of a personal nature in an email or on the internet. This includes mobile and home phone numbers, addresses, or anything else which might allow them to be identified.**
- **All emails sent should be courteous and the formality and tone of the language used appropriate to the reader. No strong or hateful language of any kind will be tolerated. Sanctions, appropriate to the case, will be imposed on any users who break this code.**

- **All emails sent from an establishment/service email account will carry a standard disclaimer disassociating the establishment/service and the Local Authority with the views expressed therein.**
- **Bullying, harassment or abuse of any kind via email will not be tolerated. Sanctions, appropriate to the case, will be imposed on any users who break this code.**
- **If users are bullied, or offensive communications are received, this must be reported immediately to a trusted adult or member of staff within school. Communications received should not be deleted, but kept for investigation purposes.**
- **Anti-virus software is used on all machines and this is regularly updated to ensure its effectiveness.**
- **Pupils will not download any files from the internet.**
- **All users will be made aware of copyright law and will acknowledge the source of any text, information or images copied from the internet.**

Procedures for Use of Social Media

- **Use of Social Media is not permitted on any school device (apart school staff accessing the school twitter account on devices agreed by the headteacher)**
- **Children, visitors, volunteers in school and staff must not access public or unregulated chat rooms/forums on school devices**

For additional information on social media use please see the acceptable use of social media guidelines

Procedures for Use of Cameras, Video Equipment and Webcams

- **Permission must be obtained from a child's parent or carer before photographs or video footage can be taken. The school uses a standard form to ensure that children have parental permission.**
- **Photographs or video footage must be downloaded immediately and saved into a designated folder. These will be accessible only to authorised members of staff. School cameras and memory cards should remain in school.**
- **Any photographs or video footage stored must be deleted immediately once no longer needed.**
- **The use of staff's own cameras, video recorders or camera phones in school or during a trip or visit is not permitted.**
- **Parents' permission must be secured in order for children to take photographs of their peers (eg – on residential visits and school trips).**
- **Webcams must not be used for personal communication and should only be used for with children in groups with an two members of staff present.**
- **Children and staff must conduct themselves in a polite and respectful manner when representing the school in a video conference or when corresponding via a webcam. The tone and formality of the language used must be appropriate to the audience and situation.**

Procedures to ensure safety of the school's website

- The school has a designated member of staff who is responsible for approving all content and images to be uploaded onto its website prior to it being published.
- The school website is subject to frequent checks to ensure that no material has been inadvertently posted, which might put children or staff at risk or cause offence.
- Copyright and intellectual property rights will be respected.
- Permission will always be obtained from parents or carers before any images of children can be uploaded onto the school website.
- Names must not be used to identify individuals portrayed in images uploaded onto the school website. Similarly, if a child or member of staff is mentioned on the website, photographs which might enable this individual to be identified must not appear.
- When photographs to be used on the website are saved, names of individuals portrayed therein should not be used as file names.

Procedures for using mobile phones

- Children who are in Year 5 and Year 6 and who walk to school and home unaccompanied are allowed to bring mobile phones to school. All children are required to switch mobile phones off and hand them into the school office on entry to school.
- The taking of still pictures or video footage with mobile phones is forbidden.
- Children should not accept files sent via Bluetooth to their mobile phones by an unknown individual. If they do (eg – on the way to school) and the content received is upsetting or makes them feel uncomfortable, they should pass this on to a trusted adult straightaway.
- The use of mobile / camera phone for inappropriate or malicious purposes (eg- for the sending of abusive or unsavoury images / text messages or files via Bluetooth, the making of hoax, crank or abusive phone calls, etc.) is forbidden and will be dealt with in accordance with the school's agreed Behaviour Policy.

Sanctions to be imposed if procedures are not followed

- The steps to be taken if rules are broken, and the types of sanctions the school intends to impose if procedures are not adhered to, include:

- Letters may be sent home to parents or carers.

- Users may be suspended from using the school's computers, internet or email, etc. for a given period of time or even indefinitely.

- Details may be passed on to the police in more serious cases.

- Legal action may be taken in extreme circumstances.

Cases of misuse will be considered on an individual basis by the headteacher and sanctions imposed to match the infringement.

Implementation of the policy

Staff are requested to report any breach of this policy to the headteacher.

Regular monitoring and recording of emails will be carried out on a monthly basis. Hard copies of emails can be used as evidence in disciplinary proceedings.

Use of the telephone system is logged and monitored.

Use of the school's internet connection is recorded and monitored.

The ICT technician checks computer logs on the school's network regularly.

Unsuccessful and successful log-ons are logged on all computers connected to the school's network.

Unsuccessful and successful software installations, security changes and items sent to the printer are also logged.

The ICT technician can remotely view or interact with any of the computers on the school's network. This may be used randomly to implement the IT Policy and to assist in any difficulties

The school's network has anti-virus software installed with a centralised administration package; any virus found is logged to this package.

The school's database systems are computerised. Unless the headteacher grants permission, users must not access the system. Failure to adhere to this requirement may result in disciplinary action.

All users of the database system will be issued with a unique individual password, which must be changed at regular intervals. This must not be disclosed to anyone.

Attempting to access the database using another employee's user account and password without prior authorisation is likely to result in disciplinary action, potentially including summary dismissal.

User accounts are accessible by the headteacher and ICT technician.

Users must ensure that critical information is not stored solely within the school's computer system. Hard copies must be kept or stored separately on the system. If necessary, documents must be password protected.

Users are required to be familiar with the requirements of the Data Protection Act 1998, and to ensure that they operate in accordance with the requirements of the Act. Employees must adhere to following rules as detailed in the act:

- **Do not disclose any material about a person, including a pupil, without their permission.**
- **Such materials that include information about person's racial or ethnic origin, sex life, political beliefs, physical or mental health, trade union membership, religious beliefs, financial matters and criminal offences will not be disclosed.**
- **Do not send any personal data outside the UK.**

This storage of data and sharing should also be in line with General Data Protection Regulation

Concluding Statement

The procedures in this policy will be subject to ongoing review and modification in order to keep up with advances in the technology coming into St Chad's and this policy will not remain static. It may be that staff and children might wish to use an emerging technology for which there are currently no procedures in place. The use of any emerging technologies will be permitted upon completion and approval of a risk assessment, which will be used to inform future policy updates.