St Chad's Primary School

E-Safety Policy

2021/22

Introduction

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

The school follows the advice and guidelines set out by the LA and the school E-Safety Policy relating to the safe use of the internet, computers, handheld devices and interactive whiteboards.

At St Chad's Church in Wales Primary School, we understand the responsibility to educate our pupils on E-Safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.
Everybody in the school has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.
Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, tablets, webcams, whiteboards, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones, camera phones, and portable media players, etc).

Acceptable Use Agreement
All pupils/ staff/ visitors will sign the appropriate Acceptable use of agreement form

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement.
However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:
Access to illegal, harmful or inappropriate images or other content

- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Rules of use are on display on the ICT display and will be placed anywhere from where children can access the internet. The children understand these rules and they know that they are expected to follow them. Should a child break these rules they will be denied internet access for a period of time after which the situation will be reviewed.

Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is used in conjunction with the School rules of 'Ready', 'Respect' and 'Safe' and with other school policies (eg behaviour, anti-bullying and child protection policies). As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

Internet Safety Day

Key e-Safety messages should be reinforced as part of the National Internet Safety day (Feb 6th 2018) (Feb 5th 2019)

The Digi-Leaders in the school are working with Eaware. A programme to teach E-Safety.

Education – pupils

The education of pupils in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

E-safety messages should be ongoing, however a PSE lesson half termly will be dedicated to embed messages using the 'Common sense' media scheme of work based on the Citizenship aspect of the DCF. The messages should then be integrated into everyday life in the school. ICT is used across the curriculum and therefore the e-safety message can be reinforced across the majority of lessons.

Technical – infrastructure / equipment, filtering and monitoring

The school and the L.A will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented.

- School ICT systems will be managed in ways that ensure that the school meets the e-safety technical requirements outlined in any relevant Local Authority E-Safety Policy and guidance
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to school ICT systems.
- All users will be provided with a username and password

Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
Appropriate security measures are present to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices.

Use of digital and video images - Photographic, Video

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 and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet/ See-Saw. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

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 eg on social networking sites.
- Staff 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. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.

- 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 without their permission
- Photographs published on the website/See-Saw, or elsewhere that include students / pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' / Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website. Pupils photos will be blurred out if parents choose for pupils not to be shown.
- Pupil's work can only be published with the permission of the pupil and parents or carers

When using communication technologies the school considers the following as good practice:
The official school email service and HWB may be regarded as safe and secure and is monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems

- Users need to be aware that email communications may be monitored
- Users must immediately report the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and pupils or parents / carers (email, chat, VLE etc) must be professional in tone and content.
- Pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

<u>Social Media</u>

- The school have recently created a closed group page on Facebook by the request of parents as another form of communication. This is closely monitored and parents have been given rules about the group.

- Staff at the school who have social media pages must at all times be professional with both their own post and liking/commenting on others. The use of using social media during the school day is not permitted whilst working with pupils. However during breaks it is advised that staff do not comment/ post on social media accounts.

The ICT subject leader will start to create an action plan based on the 360 Internet Safety Award.

January 2021

***St Chad's*"Bring Your Own Device" (BYOD)**

Responsible Use Guidelines

Purpose:

St Chad's *use digital technologies as one way of enhancing our mission to teach the skills, knowledge and behaviours students will need as responsible citizens in the global community. Students learn collaboration, communication, creativity and critical thinking in a variety of ways throughout the school day. In an effort to increase access to those 21st Century skills,* ***St Chad's*** *will allow personal devices on our guest network and school grounds for students who follow the responsibilities stated in the Acceptable Use Policy and the attached guidelines regarding BYOD.*

St Chad's *strives to provide appropriate and adequate technology to support teaching and learning. The use of personal devices by students is optional, and students who do not participate in BYOD will not be penalised and alternate modes of participation will be available.*

An important component of BYOD will be education about appropriate online behaviours. We will review cyber-safety rules with students frequently throughout the course of the school year and will offer reminders and reinforcement about safe online behaviours. In addition to the rules outlined in these guidelines, students will be expected to comply with all class and school rules while using personal devices.

Device Types:

For the purpose of this policy, the word "devices" will include: laptops, netbooks, mobile phones, smart phones, iPods, iPads, tablets, and eReaders. Please note that gaming devices with internet access are not permissible at this time.

Each pupil will be allowed to register one device to access the BYOD network.

Guidelines:

- *Pupils and parents/guardians participating in BYOD must adhere to the Internet Acceptable Use Policy and all relevant school policies.*
- *Each teacher has the discretion to allow and regulate the use of personal devices in the classroom and on specific projects.*

- *Approved devices must be in silent mode while on the school site, unless otherwise allowed by a teacher. Headphones may be used with teacher permission.*
- *Devices may not be used to cheat during tests, quizzes or exams, or for non-education purposes (such as making personal phone calls and text messaging).*
- *Pupils may not use devices to record, transmit, or post photographic images or video of a person or persons on the school site during school hours or during school activities, unless otherwise allowed by a teacher and with the consent of those persons..*
- *Devices may only be used to access content which is relevant to the classroom curriculum.*

Pupils and Parents/Guardians acknowledge that:

- *The school's network filters will be applied to a device's connection to the internet and any attempt to bypass the network filters is prohibited.*
- *Pupils are prohibited from:*
    - Bringing a device on premises that infects the network with a virus, trojan, malware or program designed to damage, alter, destroy, or provide access to unauthorized data or information.
    - Processing or accessing information on school property related to "hacking."
    - Altering or bypassing network security policies.
- *The school has the right to confiscate any device that is being used or is suspected of being used inappropriately. Parents or guardians will be contacted and arrangements made for the return of confiscated devices. BYOD privileges may well be revoked from the student.*
- *If a student's device is suspected of being used for an illegal activity or contains illegal content then the school will notify the Police and the appropriate authorities.*
- *Printing from personal devices will not be possible at school.*
- *Personal devices must be charged prior to school and run on battery power while at school. Charging of devices will not be permitted unless in exceptional circumstances (at the discretion of the school).*

Theft, Loss or Damage of Devices

It is the responsibility of each Pupil to ensure the safety and security of their Device. The School will not accept any liability for loss, damage or theft relating to Pupils' Devices (whether caused by that Pupil, other Pupils or anybody else). Pupils may wish to obtain appropriate insurance to cover their devices when on school premises.

In addition to looking after their own Devices, Pupils must ensure that their Devices are not capable of causing damage to the School's own IT equipment by having appropriate anti-virus software installed on their Devices. Furthermore, Pupils must not use their own Devices to deliberately take actions which could place the School or other Pupils at risk (such as hacking, accessing inappropriate content, downloading or using pirated software, using charged internet services, etc). Inappropriate activity of this kind will not be tolerated and may result in permission to use Pupils' Devices being withdrawn.

For the sake of clarity, Pupils should never use their Devices to:-

- *Bring the School into disrepute;*

- *Bully, intimidate or harass other Pupils, staff, visitors to the School or any other person (whether via social media, e-mail or in any other manner);*
- *Incur charges for use of online services;*
- *Access inappropriate or illegal content via the School's internet;*
- *Engage in illegal activities (such as hacking into other Devices, misusing personal information belonging to others, causing damage to School IT equipment, etc);*
- *Access the internet during lessons (unless permission is given by the class teacher);*
- *Engage in breaches of copyright laws (by either copying or supplying protected works).*

If Pupils access School data via the intranet using their own Devices, then they must ensure that this data is kept safe and not retained on their Devices for any longer than absolutely necessary. In particular, Pupils should not be retaining internal School e-mails (if received on their Devices) unless these are needed in relation to a School activity. Importantly, if a Pupil should leave this School (either to move to another school or to discontinue their education) they are expected to delete all School data from their Device immediately upon them ceasing to be a Pupil at this School.

The opportunity for Pupils to bring their own Devices into School and to use them during the school day is a privilege – not a right. If it is found that in fact, Pupils are not taking the necessary steps to secure their Devices from damage or loss, or if Pupils use their Devices in a wrongful or even criminal manner, then the School will reconsider whether it should allow Pupils to bring their own Devices and to access the internet via the School's wireless network. It is in the interests of Pupils, therefore to ensure that they abide by this policy.

Network Considerations:

Users should strive to maintain appropriate bandwidth for school-related work and communications, the school does not guarantee connectivity or the quality of the connection with personal devices. Neither the School or Wrexham CBC are responsible for maintaining or troubleshooting pupils' devices.

I understand and will abide by the above policy and guidelines. I further understand that any violation is unethical and may result in the loss of my network and/or device privileges as well as other disciplinary action. During the course of the school year, additional rules regarding the use of personal devices may be added.

_____ _____

Signature of Student *Date*

_____ _____

Signature of Parent/Guardian *Date*

St Chad's Primary School

Acceptable Use Agreement: Staff, Governors and Visitors

Acceptable Use Agreement / Code of Conduct

ICT (including data) and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school.

This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT.

All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the Headteacher.

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed acceptable by the Head or Governing Body. This also includes any media form that contains the School Name and / or logo.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role
- I will not give out my own personal details, such as mobile phone number, personal email address, personal Twitter account, or any other social media link, to pupils
- I will only use the approved, secure email system(s) for any school business
- I will ensure that personal data (such as data held on MIS software) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body. Personal or sensitive data taken off site must be encrypted, e.g. on a password secured laptop or memory stick
- I will not install any hardware or software without permission of Wrexham SRS/LA/Headteacher.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member
- Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher
- I will support the school approach to online safety and not upload or add any images, video, sounds or text linked to or associated with the school or its community
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Headteacher
- I will respect copyright and intellectual property rights
- I will ensure that my online activity, both in school and outside school, will not bring the school, my professional reputation, or that of others, into disrepute
- I will support and promote the school's e-Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies

- I will not use personal electronic devices (including smart watches) in public areas of the school between the hours of 8.30am and 3.30pm, except in the staff room and where there are areas to indicate this.

Staff at the school who have social media pages must at all times be professional with both their own post and liking/commenting on others. The use of using social media during the school day is not permitted whilst working with pupils. However during breaks it is advised that staff do not comment/ post on social media accounts.

- I understand this forms part of the terms and conditions set out in my contract of employment.

User Signature

I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school

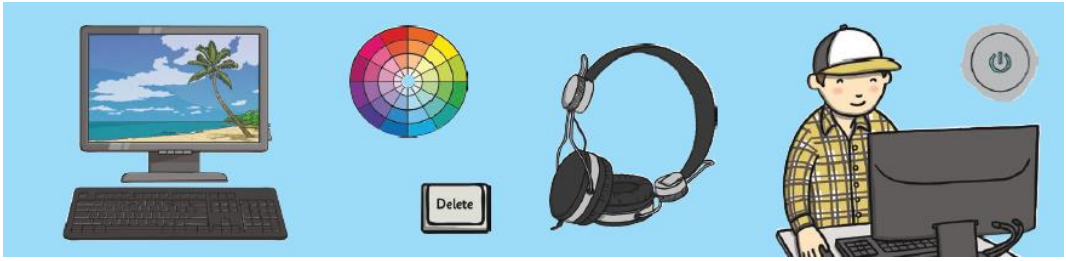
Signature …… Date ……

Full Name ……
(printed)

Job title ……

E-Safety Rules in the Foundation Phase

- Never give out your name, age, address or phone number
- Never send photographs of yourself
- Never agree to meet a stranger
- Only open emails with a teacher's help
- Tell an adult if you see something you do not like



E-Safety Rules in Key Stage Two

- Only use class or school emails
- Only open email attachments from people you know
- Use School Apps
- Don't Upload anything

- Never give out personal information
- Only open and delete your own files
- I will not say nasty things online
- If I find something unpleasant I will report it to a teacher
- I will remember that my use of ICT can be checked and a parent/ carer can be contacted if somebody is concerned about my e-safety
- I will be responsible for what I do

Dear Parents, Carers

Photographic Images of Children – Consent Form

Currently the school is working with a Web Designer, creating a new website. Photographs of the school, children etc may be published on the new website, so this letter explains why we need to ask you for your consent to any photographs of your child being taken while at school. When you have read the letter, you should fill in and return the form attached to let us know your wishes.

Generally, photographs for school and family use, and those that appear in the press, are a source of pleasure and pride. We believe they can enhance self-esteem for children and young people as well as their families and so are to be welcomed.

The use of See-Saw is very beneficial to the school and each child has a private account, where only the parent/ carer signed up will see photographs etc. There will be times where photographs of groups/ classes of children will be published and all parents can access this. Please let your class teacher know if you wish to change your consent on this issue.

In an age in which digital technology has vastly increased the use and potential misuse of photography we take the view that the risk of a child being identified by a stranger is small that, providing reasonable steps are in place in terms of school security, planning to ensure an appropriate photograph and protecting the full name and contact details of children, the practice of photography for school events by families and the media should continue, however to be mindful and responsible for posting images of other children than your own on social media etc.

The School uses the rule: “If the pupil is named, avoid using the photograph. If the photograph is used, avoid naming the pupil”. The press, however, like to reflect the local community by naming children who appear.

Please complete the form attached and return to the school office as soon as possible.
Yours sincerely,
Nicola Locker
ICT Subject Leader

CONSENT FORM – USING IMAGES OF CHILDREN

Name of Child:

Photographs of your child will be taken throughout the school day as part of learning activities etc. We may use these images in our publicity, for example in the school's prospectus or in other printed publications, as well as on our website. We may also make video recordings for school-to-school conferences, monitoring or other educational use. From time to time, our school may be visited by the media, who will take photographs or film footage.

To comply with the Data Protection Act 1998, we need your permission before we can photograph or make any recordings of your child. Please answer questions 1 to 5 below, then sign and date the form where shown.

PLEASE RETURN THE COMPLETED FORM TO THE SCHOOL AS SOON AS POSSIBLE.

Please circle yes or no as appropriate

1. May we use your child's photograph (unidentified) in the school prospectus and other printed publications that we produce for promotional purposes?

Yes No

2. May we use your child's image (unidentified) on our website?

Yes No

3. May we record your child's image (unidentified) on video?

Yes No

4. Do you consent to your child's full name being published with a press photograph? (At the present time, some local newspapers will not agree to publish a photograph without a full name.)

Yes No

Signed: …… Date: ……

Name: ……

(Parent)

Conditions of School Use

It is your responsibility to let us know if you want to withdraw or change your agreement at any time.

We, the school, will not use the personal details or full names (which means first name and surname) of any child in a photographic image on video, on our website, in our school prospectus or in any of our other printed publications. We will not include personal e-mail or postal addresses, or telephone or fax numbers on video, on our website, in our school prospectus or in other printed publications.

If we use photographs of individual pupils, we will not use the name of that child in the accompanying text or photo caption, unless we have your agreement. If we name a pupil in the text, we will not use a photograph of that child to accompany the article.

We may include pictures of pupils and teachers that have been drawn by the pupils. We may use group or class photographs or footage with very general labels, such as "a science lesson" or "making Christmas decorations". We will only use images of pupils who are suitably dressed, to reduce the risk of such images being used inappropriately.

As the child's parents/carer, we agree that if we take photographs or video recordings of our child/ren which include other pupils, we will use these for personal and family use only. I/we understand that where consent has not been obtained from the other parents for any other use, we would be in breach of the Data Protection Act 1998 if we used our recordings for any wider purpose.

Rules for Responsible Internet Use

The school has computers and iPads with Internet access to help you with your learning. These rules need to be signed before you use the Internet and will help you to keep safe and be fair to others.

Using the computers/iPads:

- I will only access the school network with the login I have been given.
- I will not try to access files in other people's folders.
- I will close all programs and log out before leaving the computer.
- I will ensure that any DVDs/USB drives that I bring in from outside school have been virus-checked before using them on the school computers.

Using the Internet:

- I will ask permission from a teacher before using the Internet.
- I will only search the Internet in ways that my teacher has approved.
- I will check who owns an image I may want to use on the Internet and will only use those with permission for re-use.
- I will minimise the web page if I find any unpleasant material and will report this to my teacher immediately because this will help protect other pupils and myself.
- I understand that the school may check my computer files, and may monitor the Internet sites I visit.

Using e-mail / messaging / forms:

- I will not give my full name, date of birth, home address or telephone number on any website.
- I will not share anyone else's personal information online.
- I will not use the Internet to arrange to meet someone outside school hours.
- I will ask permission from a teacher before sending any messages on the Internet and will only send messages to people / sites that my teacher has approved
- The messages I send will be polite and responsible.
- I will immediately report any unpleasant messages sent to me because this will help protect other pupils and myself.

Signed ……**(Child)**

……**(Parent)**

Date ……