John Clare Primary School

Inspire - Nurture – Celebrate

ICT Acceptable Use Policy

Editions and Revisions:

Reviewed	**March 2023**
Approved by FGB	**3.5.2023**
Next Review Date	**May 2024**

At John Clare Primary School we recognise that information and communication technology plays an important part in learning. All learners in school must use technology appropriately, safely and legally. We have a responsibility to make all learners aware of the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies. This policy is linked, and works alongside the school's ICT, child protection and anti-bullying policies.

Responsibility for E-safety and Appropriate use of ICT
The school governing body has responsibility for ensuring that the school has an Acceptable Use Policy for ICT and this policy is reviewed annually.

The Headteacher will ensure that there is a designated person for coordinating E-safety and acceptable use of ICT. They will work closely with the designated person for child protection.

All staff have a responsibility to use ICT appropriately and legally and report any illegal or inappropriate use of ICT to the head teacher or the designated person for e-safety, as soon as possible.

Teachers and teaching assistants should address issues of e-safety when using the internet with children. All children must follow all the ICT Code of Conduct (see appendix 2).

The ICT support team will ensure that computers have up to date virus protection and internet connection is filtered through the regional broadband consortium.

Use of the Internet
The school encourages users to make effective use of the Internet. Such use should always be lawful and appropriate. Internet usage means any connection to the Internet via Web browsing, external email or news groups.

The school expects all users to use the Internet responsibly and strictly according to the following conditions: Users shall not:

- Visit Internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:
    - pornography (including child pornography)
    - promoting discrimination of any kind
    - promoting racial or religious hatred
    - promoting illegal acts
    - any other information which may be offensive to colleagues
    - incidents which appear to involve deliberate access to Web sites, newsgroups and online groups that contain the following material will be reported to the police
    - images of child abuse involved in sexual activity or posed to be sexually provocative
    - adult material that potentially breaches the Obscene Publications Act in the UK
    - criminally racist material in the UK

If inappropriate material is accessed accidentally, users should immediately report this to the Head teacher or designated E-safety coordinator so appropriate action can be taken.

Children that access material that concerns them should follow Appendix 3.

System Monitoring & Filtering
Our broadband is provided through E2BN and all web filtering meets government standards. See Appendix 1 for procedures should and issues be raised.

All internet access provided to staff and children is strictly filtered through the broad band consortium. In addition to this we provide a comprehensive monitoring system that logs any content written, received or accessed by the user whilst on the school's system and then sends the E Safety coordinator a screen shot of that particular moment. The user will not be made aware of this unless deemed necessary. The words flagged up are linked to the Child Exploitation and Online Protection (CEOP) database and follow current word and phrasing benchmarks.

All staff and children will be made aware of the filtering when the system is implemented. In addition to its monitoring capabilities the system also provides internet logging. All access to the internet will be logged as permanent record.

Data Protection and System security

All users on the system are expected to protect their own login details as a matter of personal and system security. Under no circumstance should people allow other users to have their details or use their login. If at any time a user feels that their password has been seen by another user, they should logon and change their password immediately. It is also recommended that all passwords are alpha numeric.

User personal and system security code of conduct:

- STAFF SHOULD NEVER ALLOW CHILDREN TO LOGON USING THEIR DETAILS.
- SECURUS will monitor inappropriate use on the system. It recognises users by their user name. By allowing others to use your details you will put yourself at risk of being wrongly accused of their impropriety. It will also negate the monitoring integrity as we will not be able to guarantee that user was responsible for the inappropriate use unless we can guarantee everyone is using their login details only.
- User logon details should not be shared under any circumstances. If a student has no login report it to the office/support team for them to resolve immediately.
- When entering personal details on a website login or the platform you will often be asked if you would like to save your details. Only save your details if using your personal computer.
- The platform does contain secure student detail and staff documentation. If your details are seen by another person this data could be compromised. If in doubt change your password immediately.
- If accessing school data from home on personal or school provided hardware you should always ensure, by following the aforementioned code that data integrity is respected at all times. Your equipment is more vulnerable once it leaves the building. Laptops, mobile technology and pen drives are susceptible to theft and loss along with its data.

Digital Media

Digital media and photographs play an important part of recording events in school life. School provides iPads, laptops and Chromebooks for use by children and staff. Images of children may only be stored on the school network drives.

USB Drives

USB drives and storage devices are prohibited from use within school. Where devices, such as tablets and cameras, require a USB to operate, guidance should be sought from the Headteacher/IT support.

Staff Email

All email messages should include a standard disclaimer stating that the content of the email are not necessarily the views of school or Trust. Unsolicited email with children is not allowed. Any communication with children via email should be through the staff school email account to the pupil school account only. Do

not release or in any way make available personal details of any colleague or pupil (phone numbers, fax numbers or personal e-mail addresses) over the Internet.

Email use by children
All children will receive an email account through the use of Google Drive. The account is through an accredited school's provider and offers full filtering and security expected for student and staff use. As an online web account we cannot currently monitor use when outside the school grounds. It is possible however to monitor any emails that have been received or sent as soon as the resource is opened on the school network.

Mobile Phones
Children are not allowed mobile phones in school and should be handed to the class teacher or the school office for safekeeping if they are brought into school. Further guidance on mobile phones can be found in 'The Use of Mobile Phones in Schools Policy'.

Internet Games
There are times in the week when children have 'free' use of the school network, such as during computer clubs, wet playtimes, reward time for good behaviour etc. Any games played on the school network must be in line with the school Code of Conduct and be suitable for primary aged children.

Downloading Music
Children should not download music through the school network. If music is free to download it is usually illegal. Staff may download music but this must be done legally and in line with copyright laws.

Internet safety skills for pupils
The ICT Code of Conduct (see appendix 2) will be referred to in the Home School Agreement. The children's ICT Code of Conduct will be displayed in each classroom.

Pupils should be reminded of internet safety rules when using the Internet.

When using the internet children will be taught:

- how to critically evaluate materials
- good searching skills
- the importance of intellectual property regarding materials they find on the internet

E-safety will form part of the schools PSHE curriculum and will be taught explicitly through our use of the Natterhub programme and by using the 'Think You Know' website and resources.

Sanctions
Sanctions will be appropriate to the seriousness of the offence. For example, temporary suspension of ICT rights for minor offences, ranging to permanent exclusion and involvement of the police for very serious offences.

School website

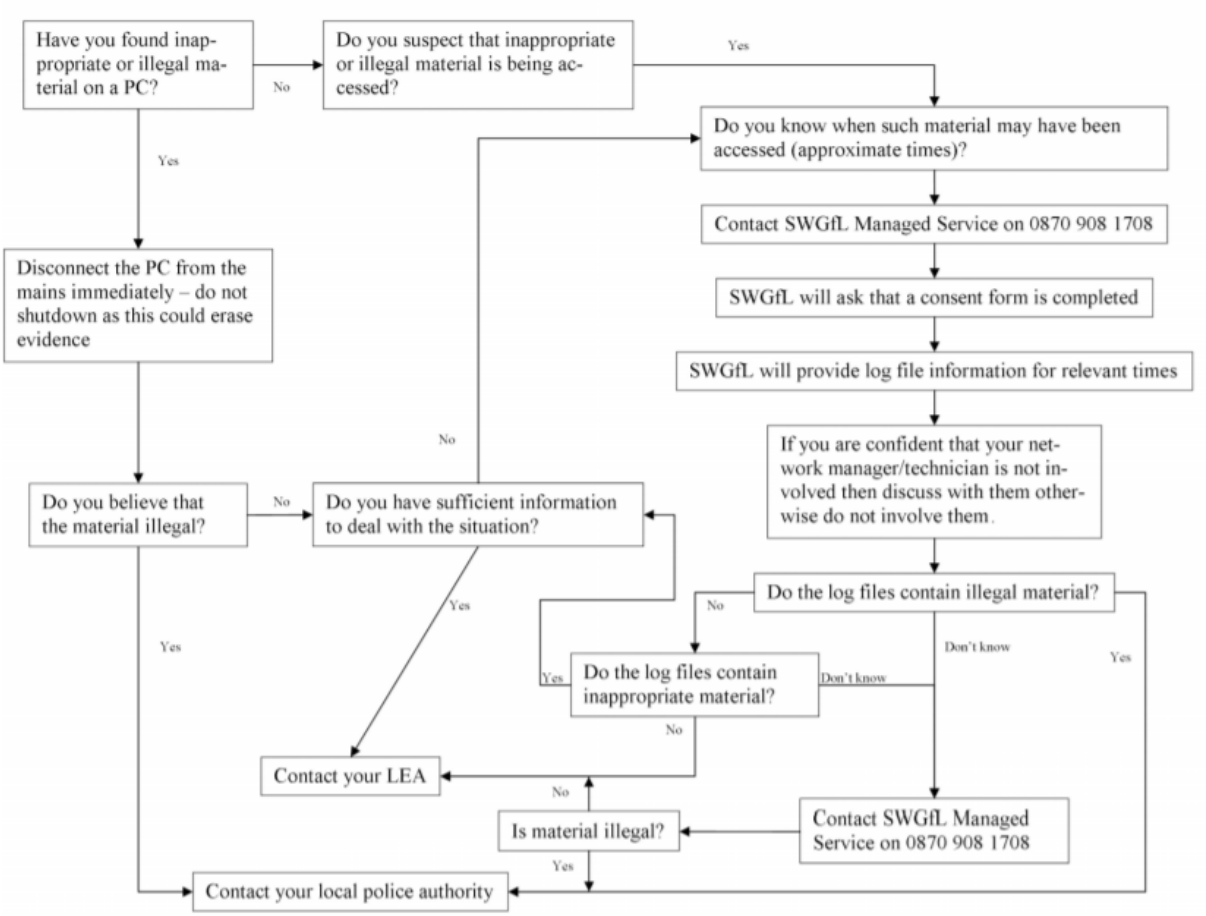
Any work published on the school website is thoroughly checked to ensure that there is no content that compromises the safety of pupils or staff.

The school will obtain parental permission before using images of pupils on the website. We ensure the image file is appropriately named – do not use pupils' names in image file names or ALT tags if published on the web. This reduces the risk of inappropriate, unsolicited attention from people outside school. We will use group photos rather than photos of individual children, wherever possible. Images will be appropriately stored and secured on the school's network.

This policy will be reviewed yearly and updated annually. It will form part of induction for all new staff.

Appendix one

This flow chart is produced by South West Grid for Learning. It will be used as a guide for senior managers on how to deal with any incident. NOTE - our contact is E2BN (telephone 01462 834588), not SWGfL as on the flowchart.



Appendix Two: Code of Conduct for Children

Always ask an adult
Only use the Internet with adult permission.

Supervision
Never use a computer without an adult present in the room. Never give anyone your personal details. Never give any information which would help anyone work out where you live or who you are. You would not give your name and address to a stranger you meet at a bus stop. So do not give your full name, telephone number or address when working on the Internet. The same applies about giving information about your family and friends.

Do not to arrange to meet people through the Internet
Remember, not everyone you 'meet' on-line are who they say they are. People can pretend to be someone else.

Do not look for things on the internet that are rude, racist or illegal
Don't reply to bad messages. If you come across things that are deliberately rude, racist, illegal or things that make you feel uncomfortable tell an adult, who will inform our service provider.

Ask 'Is it True?'
Just because it comes out of a computer does not mean it is true! Some people make up things. Always check where the information has come from and check it.

Never delete, change or read other people's e-mails, files or passwords
We share our network so remember to be careful. You do not want your work deleted or changed, so don't do it to others. Never attempt to log on as somebody else.

Do not play computer games that are not suitable for school
If you are playing games, make sure they are in line with the schools Code of Conduct – we don't have fighting in school, so don't play games that involve fighting. Don't play games which are violent or are meant for older children or adults.

Do not download or listen to music
If music is free to download, then it is usually illegal. Do not listen to music in school that is rude, racist or is meant for older children or adults.

Remember! The world is watching
Do not write things that would upset or offend other people. Others will judge you, your school and your family, by what they see on the screen.

Appendix Three: What to do if you see something that concerns you

It is likely that at some point you will come across some images or words that you did not intend to see. If this happens and you do see or hear something that scares, worries or upsets you do the following immediately:

- Turn the computer screen off! Do not turn the PC off.
- Put your hand up and ask for a teacher/adult to come straight over.
- DO NOT show other students what you have seen or discuss with them.
- Wait for someone to come over and help you quietly.
- The Teacher/adult will then tell you what to do next.