# ACCEPTABLE USE POLICY

## 1. Introduction

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Apps
- E-mail, Instant Messaging and chat rooms
- Social Media, including Facebook, Twitter, Instagram and others
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices including tablets and gaming devices
- Online Games
- Learning Platforms and Virtual Learning Environments
- Blogs and Wikis
- Podcasting
- Video sharing
- Downloading
- On demand TV and video, movies and radio / Smart TVs

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 and that some have minimum age requirements (13 years in most cases).

At Spittal Community First 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.

Schools hold personal data on learners, staff and others to help them conduct their day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in media coverage, and potentially damage the reputation of the school. This can make it more difficult for your school to use technology to benefit learners.

# ACCEPTABLE USE OF ICT POLICY

Everybody in the school community 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, regular visitors [for regulated activities] and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, mobile devices, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones and other mobile devices).

## 2. Monitoring

Authorised ICT staff may inspect any ICT equipment owned or leased by the school at any time without prior notice. If you are in doubt as to whether the individual requesting such access is authorised to do so, please ask for their identification badge and contact their department. Any ICT authorised staff member will be happy to comply with this request.

All internet activity is logged by the school's internet provider. These logs may be monitored by that provider.

## 3. Breaches

A breach or suspected breach of policy by a school employee, contractor or pupil may result in the temporary or permanent withdrawal of school ICT hardware, software or services from the offending individual.

For staff any policy breach is grounds for disciplinary action in accordance with the school Disciplinary Procedure or, for Support Staff, in their Probationary Period as stated.

Policy breaches may also lead to criminal or civil proceedings.

The Information Commissioner's powers to issue monetary penalties came into force on 6 April 2010, allowing the Information Commissioner's office to serve notices requiring organisations to pay up to £500,000 for serious breaches of the Data Protection Act.

The data protection powers of the Information Commissioner's Office are to:
• Conduct assessments to check organisations are complying with the Act;
• Serve information notices requiring organisations to provide the Information Commissioner's Office with specified information within a certain time period;
• Serve enforcement notices and 'stop now' orders where there has been a breach of the Act, requiring organisations to take (or refrain from taking) specified steps in order to ensure they comply with the law;
• Prosecute those who commit criminal offences under the Act;
• Conduct audits to assess whether organisations' processing of personal data follows good practice,

## ACCEPTABLE USE OF ICT POLICY

• Report to Parliament on data protection issues of concern

### 4. Computer Viruses

• All files downloaded from the Internet, received via e-mail or on removable media such as a memory stick must be checked for any viruses using school provided anti-virus software before being used.
• Never interfere with any anti-virus software installed on school ICT equipment.
• If your machine is not routinely connected to the school network, you must make provision for regular virus updates through your IT team.
• If you suspect there may be a virus on any school ICT equipment, stop using the equipment and contact your ICT support provider immediately. The ICT support provider will advise you what actions to take and be responsible for advising others that need to know.

### 5. Data Security

The accessing and appropriate use of school data is something that the school takes very seriously.
Security
• The school gives relevant staff access to its Management Information System, with a unique username and password
• It is the responsibility of everyone to keep passwords secure
• Staff are aware of their responsibility when accessing school data
• Staff have been issued with the relevant guidance documents and the Policy for ICT Acceptable Use
• Leadership have identified relevant responsible persons as defined in the guidance documents on the SITSS website (available - http://www.thegrid.org.uk/info/traded/sitss/)
• Staff keep all school related data secure. This includes all personal, sensitive, confidential or classified data
• Staff should avoid leaving any portable or mobile ICT equipment or removable storage media in unattended vehicles. Where this is not possible, keep it locked out of sight
• Staff should always carry portable and mobile ICT equipment or removable media as hand luggage, and keep it under your control at all times
• It is the responsibility of individual staff to ensure the security of any personal, sensitive, confidential and classified information contained in documents faxed, copied, scanned or printed. This is particularly important when shared copiers (multi-function print, fax, scan and copiers) are used

### 6. Disposal of Redundant ICT Equipment Policy

• All redundant ICT equipment will be disposed of through an authorised agency. This should include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data
• All redundant ICT equipment that may have held personal data will have the storage media over written multiple times to ensure the data is irretrievably destroyed. Or if the storage media has failed it will be physically destroyed. We will only use authorised companies who will supply a written guarantee that this will happen
• Disposal of any ICT equipment will conform to:

# ACCEPTABLE USE OF ICT POLICY

The Waste Electrical and Electronic Equipment Regulations 2006
The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007
http://www.environment-agency.gov.uk/business/topics/waste/32084.aspx
http://www.opsi.gov.uk/si/si2006/uksi_20063289_en.pdf
http://www.opsi.gov.uk/si/si2007/pdf/uksi_20073454_en.pdf?lang=_e
Data Protection Act 1998 https://ico.org.uk/for-organisations/education/
 General Data Protection Regulations 2018 (GDPR) https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/
Electricity at Work Regulations 1989
http://www.opsi.gov.uk/si/si1989/Uksi_19890635_en_1.htm

The school will maintain a comprehensive inventory of all its ICT equipment including a record of disposal
• The school's disposal record will include:
• Date item disposed of
• Authorisation for disposal, including:
• verification of software licensing any personal data likely to be held on the storage media?
* How it was disposed of eg waste, gift, sale Name of person & / or organisation who received the disposed item * if personal data is likely to be held the storage media will be over written multiple times to ensure the data is irretrievably destroyed.
• Any redundant ICT equipment being considered for sale / gift will have been subject to a recent electrical safety check and hold a valid PAT certificate

## 7. E-mail

The use of e-mail within most schools is an essential means of communication for both staff and pupils. In the context of school, e-mail should not be considered private. Educationally, e-mail can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school or international. We recognise that pupils need to understand how to style an e-mail in relation to their age and how to behave responsible online.

**Managing e-mail**
• The school gives all staff their own e-mail account to use for all school business as a work based tool This is to protect staff, minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed
• Staff should use their school email for all professional communication.
• It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary e-mail histories can be traced. The school email account should be the account that is used for all school business
• Under no circumstances should staff contact pupils, parents or conduct any school business using personal e-mail addresses
• All e-mails should be written and checked carefully before sending, in the same way as a letter written on school headed paper

# ACCEPTABLE USE OF ICT POLICY

• Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes
• E-mails created or received as part of your school job will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000. You must therefore actively manage your e-mail account as follows:
– Delete all e-mails of short-term value
 – Organise e-mail into folders and carry out frequent house-keeping on all folders and archives

## 8.  Equal Opportunities
### Pupils with Additional Needs
The school endeavours to create a consistent message with parents/carers for all pupils and this in turn should aid establishment and future development of the schools' eSafety rules. However, staff are aware that some pupils may require additional support or teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of eSafety issues. Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of eSafety. Internet activities are planned and well managed for these children and young people.

## 9.  Managing Other Online Technologies
Online technologies, including social networking sites, if used responsibly both outside and within an educational context can provide easy to use, creative, collaborative and free facilities. However it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our pupils to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

• At present, the school endeavors to deny access to social networking and online games websites to pupils within school
• All pupils are advised to be cautious about the information given by others on such websites, for example users not being who they say they are
• Pupils are taught to avoid placing images of themselves (or details within images that could give background details) on such websites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online
• Pupils are always reminded to avoid giving out personal details on websites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, IM/ email address, specific hobbies/ interests)
• Our pupils are advised to set and maintain their online profiles to maximum privacy and deny access to unknown individuals
• Pupils are encouraged to be wary about publishing specific and detailed private thoughts and information online
• Our pupils are asked to report any incidents of Cyberbullying to the school
• Staff may only create blogs, wikis or other online areas in order to communicate with pupils using the school learning platform or other systems approved by the Headteacher

# ACCEPTABLE USE OF ICT POLICY

• Services such as Facebook and Instagram have a 13+ age rating which should not be ignored
http://www.coppa.org/comply.htm

### 10.    Safe Use of Images
**Taking of Images and Film**
Digital images are easy to capture, reproduce and publish and, therefore, misuse. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.
• With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment

**Publishing Pupil's Images and Work**
On a child's entry to the school, all parents/carers will be asked to give permission to use their child's work/photos in the following ways:
 • on the school web site
• in the school prospectus and other printed publications that the school may produce for promotional purposes
• recorded/ transmitted on a video or webcam
• on the school's learning platform or Virtual Learning Environment
• in display material that may be used in the school's communal areas
• in display material that may be used in external areas, ie exhibition promoting the school
• general media appearances, eg local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, eg divorce of parents, custody issues, etc.
Parents or carers may withdraw permission, in writing, at any time. Consent must also be given in writing and will be kept on record by the school.
Pupils' names will not be published alongside their image and vice versa. E-mail and postal addresses of pupils will not be published.
Pupils' full names will not be published. Before posting student work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed.

### 11.    School ICT Equipment including Portable & Mobile ICT Equipment & Removable Media
School ICT Equipment
• As a user of the school ICT equipment, you are responsible for your activity
• It is recommended that schools log ICT equipment issued to staff and record serial numbers as part of the school's inventory
• Do not allow your visitors to plug their ICT hardware into the school network points (unless special provision has been made). They should be directed to the wireless ICT facilities if available
• Ensure that all ICT equipment that you use is kept physically secure

# ACCEPTABLE USE OF ICT POLICY

• Do not attempt unauthorised access or make unauthorised modifications to computer equipment, programs, files or data. This is an offence under the Computer Misuse Act 1990 •
It is imperative that you save your data on a frequent basis to the school's network. You are responsible for the backup and restoration of any of your data that is not held on the school's network

• Personal or sensitive data should not be stored on the local drives of desktop PC, laptop, USB memory stick or other portable device. If it is necessary to do so the local drive must be encrypted

• It is recommended that a time locking screensaver is applied to all machines. Any device accessing personal data must have a locking screensaver as must any user profiles

• Privately owned ICT equipment should not be used on a school network

• On termination of employment, resignation or transfer, return all ICT equipment to your Manager. You must also provide details of all your system logons so that they can be disabled

• It is your responsibility to ensure that any information accessed from your own PC or removable media equipment is kept secure, and that no personal, sensitive, confidential or classified information is disclosed to any unauthorised person

• All ICT equipment allocated to staff must be authorised by the appropriate Line Manager. Authorising Managers are responsible for:

o maintaining control of the allocation and transfer within their unit

o recovering and returning equipment when no longer needed

• All redundant ICT equipment is disposed of in accordance with Waste Electrical and Electronic Equipment (WEEE) directive and Data Protection Act (DPA)

## Portable & Mobile ICT Equipment

This section covers such items as laptops, mobile devices and removable data storage devices. Please refer to the relevant sections of this document when considering storing or transferring personal or sensitive data

• All activities carried out on school systems and hardware will be monitored in accordance with the general policy

• Staff must ensure that all school data is stored on the school network, and not kept solely on the laptop. Any equipment where personal data is likely to be stored must be encrypted

• Equipment must be kept physically secure in accordance with this policy to be covered for insurance purposes. When travelling by car, best practice is to place the laptop in the boot of your car before starting your journey

• Synchronise all locally stored data, including diary entries, with the central school network server on a frequent basis

• Ensure portable and mobile ICT equipment is made available as necessary for anti-virus updates and software installations, patches or upgrades

• The installation of any applications or software packages must be authorised by the ICT support team, fully licensed and only carried out by your ICT support

• In areas where there are likely to be members of the general public, portable or mobile ICT equipment must not be left unattended and, wherever possible, must be kept out of sight

• Portable equipment must be transported in its protective case if supplied

# ACCEPTABLE USE OF ICT POLICY

## Mobile Technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Mobile technologies such Smartphones, Blackberries, iPads, games players, are generally very familiar to children outside of school. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

## 12. Personal Mobile Devices (including phones)

The school allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the school allow a member of staff to contact a pupil or parent/ carer using their personal device The school is not responsible for the loss, damage or theft of any personal mobile device The sending of inappropriate text messages between any member of the school community is not allowed Permission must be sought before any image or sound recordings are made on these devices of any member of the school community Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device

## 13. School Provided Mobile Devices (including phones and iPads)

• The sending of inappropriate text messages between any member of the school community is not allowed
• Permission must be sought before any image or sound recordings are made on the devices of any member of the school community
• Where the school provides mobile technologies such as phones, laptops and iPads for offsite visits and trips, only these devices should be used
• Where the school provides a laptop for staff, only this device may be used to conduct school business outside of school
• Never use a hand-held mobile phone whilst driving a vehicle

## 14. Social Media, including Facebook and Twitter

Facebook, Twitter and other forms of social media are increasingly becoming an important part of our daily lives.
• Staff are not permitted to access their personal social media accounts using school equipment at any time/ during from school during school hours
• Pupils are not permitted to access their social media accounts whilst at school
• Staff, governors, pupils, parents and carers are aware that the information, comments, images and video they post online can be viewed by others, copied and stay online forever
• Staff, governors, pupils, parents and carers are aware that their online behaviour should at all times be compatible with UK law

## 15. Systems and Access

• You are responsible for all activity on school systems carried out under any access/account rights assigned to you, whether accessed via school ICT equipment or your own PC

# ACCEPTABLE USE OF ICT POLICY

- Do not allow any unauthorised person to use school ICT facilities and services that have been provided to you
- Ensure you remove portable media from your computer when it is left unattended
- Use only your own personal logons, account IDs and passwords and do not allow them to be used by anyone else
- Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information
- Ensure you lock your screen before moving away from your computer during your normal working day to protect any personal, sensitive, confidential or otherwise classified data and to prevent unauthorised access
- Ensure that you logoff from the PC completely when you are going to be away from the computer for a longer period of time
- Do not introduce or propagate viruses
- It is imperative that you do not access, load, store, post or send from school ICT any material that is, or may be considered to be, illegal, offensive, libelous, pornographic, obscene, defamatory, intimidating, misleading or disruptive to the school or may bring the school or HCC into disrepute. This includes, but is not limited to, jokes, chain letters, files, emails, clips or images that are not part of the school's business activities; sexual comments or images, nudity, racial slurs, gender specific comments, or anything that would offend someone on the basis of their age, sexual orientation, religious or political beliefs, national origin, or disability (in accordance with the Sex Discrimination Act, the Race Relations Act and the Disability Discrimination Act)
- Any information held on School systems, hardware or used in relation to School business may be subject to The Freedom of Information Act
- Where necessary, obtain permission from the owner or owning authority and pay any relevant fees before using, copying or distributing any material that is protected under the Copyright, Designs and Patents Act 1998
- It is essential that any hard drives which may have held personal or confidential data are 'scrubbed' in way that means the data can no longer be read. It is not sufficient to simply delete the files or reformat the hard drive. Whoever you appoint to dispose of the equipment must provide a written guarantee that they will irretrievably destroy the data by multiple over writing the data.

# ACCEPTABLE USE OF ICT POLICY

## Pupil Acceptable Use
## Agreement / e-Safety Rules

- I will only use ICT in school for school purposes
- I will only use my class e-mail address or my own school e-mail address when e-mailing
- I will only open e-mail attachments from people I know, or who my teacher has approved
- I will not tell other people my ICT passwords
- I will only open/delete my own files
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible
- I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this, I will tell my teacher immediately
- I will not give out my own/others details such as name, phone number or home address. I will not arrange to meet someone or send my image unless this is part of a school project approved by my teacher and a responsible adult comes with me
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community
- I know that my use of ICT can be checked and my parent/carer contacted if a member of school staff is concerned about my safety
- I will not sign up for any online service unless this is an agreed part of a school project approved by my teacher

**Spittal Community First School**

Dear Parent/ Carer

ICT including the internet, e-mail and mobile technologies has become an important part of learning in our school. We expect all children to be safe and responsible when using any ICT. Please read and discuss these eSafety rules with your child and return the slip at the bottom of this page. If you have any concerns or would like some explanation please contact Mrs Kiff.

Please take care to ensure that appropriate systems are in place at home to protect and support your child/ren.

∀ Parent/ carer signature We have discussed this document with

………………………………………..(child's name) and we agree to follow the eSafety rules and to support the safe use of ICT at Spittal Community First School.

Parent/ Carer Signature …………………………………………………….

Class ………………………………. Date ………………………………

# ACCEPTABLE USE OF ICT POLICY

## Staff, Governor and Visitor
## Acceptable Use Agreement / Code of Conduct


ICT (including data) and the related technologies such as e-mail, 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 Mrs Kiff.


• 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
• 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 e-mail address, personal Twitter account, or any other social media link, to pupils
• I will only use the approved, secure e-mail 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, eg on a password secured laptop or memory stick
• I will not install any hardware or software without permission of Mrs Kiff
• 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 deliberately upload or add any images, video, sounds or text that could upset any member of the school 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 role or that of others into disrepute
• I will support and promote the school's e-Safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies


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 …………………………………………….

# ACCEPTABLE USE OF ICT POLICY

Chair of Governor Committee

Signed:………………………………………………

Print Name: ……………………………………… Date:…………………………………

Head teacher

Signed: ………………………………………….

Print name: ……………………………………… Date:………………………………….

REVIEW DATE : Summer 2023