“Each one of you is a child of God” Pope Francis

All Saints is educating for Unity, Responsibility, Courage, Wisdom and Generosity

ICT Acceptable Use Policy

PURPOSE

The policy defines and describes the acceptable use of ICT (Information and Communications Technology) and mobile phones for All Saints School staff and students. Its purpose is to safeguard against computer and mobile phone misuse, to protect staff, students and the school from possible litigation, to minimise the risk to ICT systems and to minimise the risk to pupils from inappropriate or unwanted contact from others.

SCOPE

This policy deals with the use of ICT facilities in schools and applies to all school-based employees, students and other authorised users, e.g. contractors, volunteers etc.

SCHOOL RESPONSIBILITIES

The Governing Body is responsible for ensuring that its employees act in a lawful manner, making appropriate use of school technologies for approved purposes only.

Automated systems have been implemented on school ICT systems to proactively detect computer misuse within classrooms, on laptops and on PCs in school open areas.

The Governing Body is responsible for adopting relevant policies and the Headteacher for ensuring that staff, students and parents are aware of their contents.

Where staff are concerned, if the Headteacher has reason to believe that any ICT equipment has been misused. Incidents will be investigated in a timely manner in accordance with agreed procedures.

The Headteacher should make it clear that internal school staff should not carry out any investigations unless they are both qualified and authorised to do so.

Access to School ICT equipment, e-mail services and the Internet will not be granted until a signed ***Acceptable Use of ICT Policy*** declaration is received and filed.

USER RESPONSIBILITIES

Staff found to be in breach of this policy may be disciplined in accordance with the disciplinary procedure. In certain circumstances, breach of this policy may be considered gross misconduct resulting in termination of employment. Users must report all suspected breaches of this policy to the Headteacher.

Students found to be in breach of this policy may be disciplined in accordance with the school's disciplinary procedure. In certain circumstances, breach of this policy may be considered gross breach of school discipline resulting in either temporary or permanent exclusion. Users must report all suspected breaches of this policy to a responsible member of staff.

By signing the Acceptable Use of ICT Policy declaration.

All users are expected to act in a responsible, ethical and lawful manner with the understanding that school electronic and manual information may be accessible to the public under the Freedom of Information Act 2000. Users should uphold privacy and confidentiality in accordance with the Data Protection Act 1998. Care must also be taken not to breach another person's copyright, trademark or design, nor to publish any defamatory content.

Staff and students will be held liable for the cost of repair or replacement of ICT equipment that is damaged or rendered unusable through negligence, misuse, or failing to take adequate precautions or reasonable care, to prevent damage or equipment failure.

Staff and students must follow authorised procedures when relocating ICT equipment or taking mobile devices offsite. It is essential that any personal information or data held on a PC, laptop, memory stick, cd, DVD or any other storage device is safeguarded appropriately, particularly when taken off site. All data which is private or confidential, whether processed or not must be encrypted to prevent unauthorised access.

Users are required to protect and keep secret their password(s) and not share their account details, particularly passwords with others nor use another individual's account or misrepresent their identity by doing so for any reason. ***Users must not under any circumstances reveal their password to anyone else.***

Staff must not, under any circumstances allow students or other *unauthorised* persons (e.g. contractors, temporary workers etc.) to use their laptops, notebook or designated teacher/admin work stations under any circumstances. If contractors or temporary workers require ICT access this should arranged by the ICT Co-Ordinator.

No user shall access (e.g., read, write, modify, delete, copy, move) another user's personal electronic documents (including email) without the owner's permission or as allowed by this policy or by law.

Users must not download or install ***executable*** software (including but not limited to .exe files, flash games or movies, mpeg and wmv files) on any device, including USB devices.

Periodic audits of software held on ICT equipment will be undertaken. All unauthorised ***executable*** software will be deleted from school ICT systems without notice.

Users must take care to store sensitive information, e.g. pupil or staff information, safely and to keep it password protected, on all school systems, including laptops. If student or staff data is extract, processed (converted to CSV or other readable file type) then copied from a secure school system to removable media (CD, DVD, memory stick etc.), the data ***must be encrypted*** to prevent unauthorised access.

Network connected devices must have school approved anti-virus software installed and activated. Users may not turn off anti-virus software. All users of ICT resources have the responsibility to take precautions to prevent the initial occurrence and subsequent spreading of a computer virus. No one may knowingly create, install, run, or distribute any malicious code (e.g. viruses, Trojans, worms) or another destructive program on any ICT resource.

It is the ***user's*** responsibility to ensure that appropriate antivirus precautions are taken when using removable media.

No one may knowingly or willingly interfere with the security mechanisms or integrity of ICT resources. No one may use ICT resources to attempt unauthorised use, or interfere with the legitimate use by authorised users, of other computers on internal or external networks. Access to networks will be monitored.

Staff and students must not under any circumstances attempt to access the school's wireless or wired networks without the written approval of the ICT Co-Ordinator. Any attempt to "hack" into either the wireless or wired networks will be considered gross misconduct.

Within the terms of the Data Protection Act 1998, Human Rights Act 1998 and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, the County Council or school may record or inspect any information transmitted through or stored in its computers, including e-mail communications and individual login sessions, without notice when:

- There is reasonable cause to believe the user has violated or is violating this policy, any guidelines or procedures established to implement this policy.
- The *Secures* system has detected inappropriate or unusual activity

- An account appears to be engaged in unusual or unusually excessive activity.
- It is necessary to do so to protect the integrity, security, or functionality of ICT resources or to protect the County Council or its partners from liability.
- Establishing the existence of facts relevant to the business.

- Ascertaining or demonstrating standards which ought to be achieved by those using the ICT facilities.
- Preventing or detecting crime Investigating or detecting unauthorised use of ICT facilities
- Ensuring effective operation of ICT facilities, determining if communications are relevant to the business (for example, in the last resort where an employee is off sick or on holiday and business continuity is threatened) it is otherwise permitted or required by law.

Staff and Students must not send private, sensitive or confidential data or information by unencrypted email, electronic file transfer or by using removable media - particularly to an external recipient - if accidental disclosure could lead to significant harm or embarrassment to an individual, the school personal data where possible e.g. by using initials. Use passwords on sensitive documents that must be sent to external recipients.

Websites or sub websites should not be created on school equipment without the written permission of the Headteacher or the ICT.

No one may use ICT resources to transmit abusive, threatening, or harassing material, chain letters, spam, or communications prohibited by law. No one may abuse the policies of any newsgroups, mailing lists, and other public forums through which they participate from a school account.

The following content should not be created or accessed on ICT equipment at any time:

- Material that gratuitously displays images of violence, injury or death
- Material that is likely to lead to the bullying or harassment of others
- Material that promotes intolerance and/or discrimination on grounds of race, sex, disability, sexual orientation, religion or age
- Material relating to criminal activity, e.g. buying and selling illegal drugs
- Material relating to any other unlawful activity e.g. breach of copyright
- Material that may generate security risks and encourage computer misuse
- Social network sites that allow the creation of personal web space or allow the storage of private and personal information, pictures and/or videos e.g. Bebo.com, FaceBook.com, MySpace, Twitter etc., or could bring school into disrepute.
- Computer games sites, flash games (whether on-line or stored on local/network drives) etc.
- Betting or on-line gambling sites (e.g. casinos, horse racing, bookies etc.)
- Proxy server sites designed to bypass school security protocols and/or ICT policies or that provides unauthorised or anonymous access to web based or other services.
- Any form on on-line purchasing unless it has been approved by the ICT Coordinator and guaranteed against fraudulent transactions.
- Any content that is deemed to be on a non-educational or non-business nature except where allowed under the ***Personal Use and Privacy*** section of this document.

In addition to the above staff and students must not under circumstances engage in activities using ICT equipment or services (including but not limited to e-mail services, messaging services, collaboration or social networking sites, message, bulletin or other forum sites that could be considered:

- Racist, intolerant, discriminatory, bullying or harassment of an individual, group or institution
- Inappropriate or contrary to the expected high standards of professionalism in any way
- Detrimental, provocative or defamatory to an individual, group or institution
- Critical of School its' students, staff, parents, governors or other stake holders

As a concession to the above rules ***Teachers and Teaching Assistants*** are allowed to access ***youtube.com*** to facilitate learning and teaching. No other member of staff should access this site.

At no time should staff or students directly or indirectly present their personal opinions as those of School.

It is possible to access or be directed to unacceptable Internet sites by accident. These sites can be embarrassing, will leave an audit trail on both host PC and on Secures and such sites can be difficult to get out of. If staff or students have accessed unacceptable content or are in receipt of unacceptable material via email, they should inform the Headteacher or the ICT Co-Ordinator immediately. This may avoid problems later should monitoring systems be alerted to the content.

Staff should not open unsolicited external e-mails, particularly where the sender cannot be easily identified or where the subject line is nebulous, unexpected or out of context with current duties. All such incidences should be reported to either the Head Teacher or the ICT Co-Ordinator.

PERSONAL USE & PRIVACY

In the course of normal operations, ICT resources are to be used for business or curriculum purposes only. The school permits limited personal use of ICT facilities by authorised users subject to the following limitations:

- Personal use must be in the ***user's own time*** and must not impact upon teaching/work efficiency or costs.
- The level of use must be reasonable and not detrimental to the main purpose for which the facilities are provided.
- Personal use must not be of a commercial or profit-making nature.
- Personal use must not be of a nature that competes with the business of the school or conflicts with an employee's or student's obligations.
- Computer games must not be installed, downloaded, or played from the internet or stored in any form on school ICT equipment.
- Music files and video content (e.g. MP3, MP4, WMV, MPEG, and DVI etc.) must not be downloaded, stored or used on school ICT equipment unless the appropriate copyright protocols have been adhered to and they are for learning and teaching purposes.

Personal use of the Internet must not involve attempting to access the categories of content described in the **Users Responsibilities** section above, regardless of whether it is normally automatically blocked by web filtering software or not.

USE OF DIGITAL AND VIDEO IMAGES – PHOTOGRAPHIC AND VIDEO

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff and students need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees.

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 students 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 e.g. on social networking sites.
- Staff is 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.
- All digital and/or video images must be stored in a secure location and NOT on shared cameras. Images should be removed from shared digital/video cameras once individual photographic or video sessions are completed.
- Care should be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the school's website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' 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 students are published on the school website (this may be covered as part of the AUP signed by parents or carers at the start of the year see.
- Student's work can only be published with the permission of the student / pupil and parents or carers.

SECURE STORAGE OF AND ACCESS TO DATA

The school will ensure that ICT systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them.

All users will be given secure user names and strong passwords which must be changed every six weeks. User names and passwords must never be shared.

Personal data may only be accessed on machines that are securely password protected. Any device that can be used to access data must be locked if left (even for very short periods) and set to auto lock if not used for five minutes.

All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.

Personal data can only be stored on school equipment (this includes computers and portable storage media) (where allowed). Private equipment (i.e. owned by the users) must not be used.

When personal data is stored on any portable computer system, USB stick or any other removable media:

- The data must be encrypted and password protected.
- The device must be password protected (many memory sticks / cards and other mobile devices cannot be password protected).
- The device must offer approved virus and malware checking software.
- The data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

The school recognises that under Section 7 of the Data Protection Act, data subjects have a number of rights in connection with their personal data, the main one being the right of access. Procedures are in place to deal with Subject Access Requests i.e. a written request to see all or a part of the personal data held by the data controller in connection with the data subject. Data subjects have the right to know: if the data controller holds personal data about them; a description of that data; the purpose for which the data is processed; the sources of that data; to whom the data may be disclosed; and a copy of all the personal data that is held about them. Under certain circumstances the data subject can also exercise rights in connection with the rectification; blocking; erasure and destruction of data.

SECURE TRANSFER OF DATA AND ACCESS OUTSIDE OF SCHOOL

The school recognises that personal data may be accessed by users out of school, or transferred to the LA or other agencies. In these circumstances:

- Users may not remove or copy sensitive or personal data from the school or authorised premises without permission and unless the media is encrypted and password protected and is transported securely for storage in a secure location.
- Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (e.g. family members) when out of school.
- When data is required by an authorised user from outside the school premises (for example, by a teacher or student working from their home or a contractor) they must have secure remote access to the management information system (MIS) or learning platform.
- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software.
- Particular care should be taken if data is taken or transferred to another country, particularly outside Europe, and advice should be taken from the local authority in this event. (nb. to carry encrypted material is illegal in some countries)

The school will comply with the requirements for the safe destruction of personal data when it is no longer required.

MOBILE PHONE COMMUNICATION AND INSTANT MESSAGING

Staff are advised not to give their home telephone number or their mobile phone number to pupils. Mobile phone communication should be used sparingly and only when deemed necessary.

Staff are advised not to make use of pupils' mobile phone numbers either to make or receive phone calls or to send to or receive from pupil's text messages other than for approved school business.

If mobile phone voice or text communication is established with a student because of educational necessity, the following guidelines must be followed:

- The staff member's line Co-Ordinator must be informed in writing in advance.
- Student's parents or guardians must be informed in writing in advance.

Photographs and videos of pupils should not be taken with mobile phones.

Photographs and videos of staff should not be taken with mobile phones.

Staff should only communicate electronically with pupils from school accounts on approved school business, e.g. coursework.

Staff should not enter into instant messaging communications with pupils.

Student's use of mobile telephones is restricted and the following rules MUST be followed:

- Mobile phones are not to be used in the main school building during the school day.
- Students must not photograph members of staff using their mobile phones or any other mobile device.
- Students must not take photographs of each other as they could be used for any inappropriate purpose what so ever.

A confiscated mobile phone will be placed in a secure cabinet in the office area and students can collect them at the end of the school day from a member of the office team.

LEGISLATION

All users (staff, students and contractors) should be aware of the legislative framework under which this Policy and guidance has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

It is recommended that legal advice is sought in the advent of an e safety issue or situation.

Computer Misuse Act 1990

This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- "Eavesdrop" on a computer;
- Make unauthorised use of computer time or facilities; maliciously corrupt or erase data or programs; Deny access to authorised users.

IMPORTANT LEGAL NOTICE

The provision of internet and e-mail facilities to staff and students is entirely at School's discretion and may be withdrawn or suspended without notice. School shall not be liable for any claims or losses of any nature arising from the inappropriate use of ICT equipment or misuse of the internet or e-mail services (except by the extent required by law).

Links with policies

This document should be read in conjunction with the following school policies available on the school website:

- Behaviour policy
- Safeguarding policy
- Data Protection (GDPR) policy
- ICT Acceptable Use policy
- Mobile Phone Policy
- Remote Learning Document