ALL SAINTS' C.E. PRIMARY SCHOOL, ALREWAS
E- SAFETY POLICY STATEMENT

'Believe to Achieve'
"Living life to the full" (John 10:10)

School Values
Love + Forgiveness + Friendship + Thankfulness + Trust + Respect = Koinonia

With the teachings of Jesus as our guide, we embrace a creative and ambitious curriculum to ignite a passion for learning. We prepare our children for a rapidly changing world by equipping them with critical and creative thinking skills, independence, resilience and respect for our core school values.

Introduction

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
- ✓ E-mail and Instant Messaging
- ✓ Chat Rooms and Social Networking
- ✓ Blogs and Wikis
- ✓ Podcasting
- ✓ Video Broadcasting
- ✓ Music Downloading
- ✓ Gaming
- ✓ Mobile/ Smart phones with text, video and/ or web functionality
- ✓ Other mobile devices with web functionality

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.

At this school, we understand the responsibility to educate our children 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.

Both this policy and the Acceptable Use Agreement are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, tablets, whiteboards, voting systems, digital video equipment, etc); and technologies owned by children and staff, but brought onto school premises (such as laptops, mobile phones, camera phones, tablets and portable media players, etc).

Monitoring

Authorised ICT staff (ICT Technician), Headteacher or Data Protection Officer may inspect any ICT equipment owned or leased by the School at any time without prior notice.

ICT authorised staff may monitor, intercept, access, inspect, record and disclose telephone calls, e-mails, instant messaging, internet/intranet use and any other electronic communications (data, voice or image) involving its employees or contractors, without consent, to the extent permitted by law. This may be to confirm or obtain School business related information; to confirm or investigate compliance with School policies, standards and procedures; to ensure the effective operation of School ICT; for quality control or training purposes; to comply with a Subject Access Request under the General Data Protection Register 2018 (GDPR), or to prevent or detect crime.

All monitoring, surveillance or investigative activities are conducted by ICT authorised staff and comply with the General Data Protection Register 2018 (GDPR), the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000.

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.

Any policy breach is grounds for disciplinary action in accordance with the School Disciplinary Procedure or, where appropriate, the LA Disciplinary Procedure or Probationary Service Policy. Policy breaches may also lead to criminal or civil proceedings.

Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's DPO or Headteacher. Additionally, all security breaches, lost/stolen equipment or data (including USB flash pens), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the DPO and Headteacher with immediate effect (within 24 hours).

Computer Viruses

All files downloaded from the Internet, received via e-mail or on removable media (e.g. USB stick) must be checked for any viruses using school provided anti-virus software before using them.

Security

It is the responsibility of everyone to keep passwords secure.

Staff are aware of their responsibility when accessing school data.

Staff should avoid leaving any portable or mobile ICT equipment or removable storage media in unattended vehicles. Where this is not possible, it is kept locked out of sight.

It is the responsibility of individual staff to ensure the security of any personal, sensitive, confidential and classified information contained in documents, copied, scanned or printed. This is particularly important when shared copiers (multi-function print, scan and copiers) are used.

Impact Levels and Protective Marking

Appropriate labelling of data should help schools secure data and so reduce the risk of security incidents. Our school uses the following coding :

Unclassified	Personal (protect)	Sensitive (official/restrict)

Apply labelling in accordance with guidance from your Data Protection Officer (DPO).
The sensitivity of an asset may change over time and it may be necessary to reclassify assets. If a document is being de-classified or the marking changed, the file should also be changed to reflect the highest marking within its contents.
Reviews are continuing to look at the practical issues involved in applying protective markings to electronic and paper records and government representatives are working with suppliers to find ways of automatically marking reports and printouts.

Data Protection Officer (DPO)

The DPO in this school is through the Local Authority – see policy.

The role of the DPO is to understand:

- what information is held, and for what purposes
- what information needs to be protected (e.g. any data that can be linked to an individual, pupil or staff etc including UPN, teacher DCSF number etc)
- how information will be amended or added to over time
- who has access to the data and why
- how information is retained and disposed of

As a result, the DPO is able to manage and address risks to the information and make sure that information handling complies with legal requirements laid down in the GDPR (2018).
Although these roles have been explicitly identified, the handling of secured data is everyone's responsibility – whether they are an employee, consultant, software provider or managed service provider. Failing to apply appropriate controls to secure data could amount to gross misconduct or even legal action.

Disposal of Redundant ICT Equipment Policy

Some redundant ICT equipment will be disposed of through an authorised agency or via LA disposal scheme. This should include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.
Some 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:
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

General Data Protection Register 1998
http://www.ico.gov.uk

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 comply with the up to date guidance and be within the delegated limits as defined by the schools Governors

Further information is available at:
Waste Electrical and Electronic Equipment (WEEE) Regulations Environment Agency web site Introduction

http://www.environment-agency.gov.uk/business/topics/waste/32084.aspx

The Waste Electrical and Electronic Equipment Regulations 2006

http://www.opsi.gov.uk/si/si2006/uksi_20063289_en.pdf

The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007

http://www.opsi.gov.uk/si/si2007/pdf/uksi_20073454_en.pdf?lang=_e

Information Commissioner website
http://www.ico.gov.uk/

Managing e-Mail
The school gives teaching staff their own e-mail account to use for all school business as a work based tool. This is to minimise the risk of receiving unsolicited or malicious e-mails and avoids the risk of personal profile information being revealed.
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 children, parents, clients or conduct **ANY** school business using personal e-mail addresses.
The school requires a standard disclaimer to be attached to all e-mail correspondence, stating that, 'the views expressed are not necessarily those of the school or the LA'. The responsibility for adding this disclaimer lies with the account holder as follows:

Confidentiality: *This email and its contents and any attachments are intended only for the above named. As the email may contain confidential or legally privileged information, if you are not, or suspect that you are not, the above named or the person responsible for delivery of the message to the above named, please delete or destroy the email and any attachments immediately.*

Governors, trustees or directors should ensure that they **ONLY** use the provided school e-mail address when communicating on school related business.
Children 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.
Staff must inform (the DPO or Headteacher) if they receive an offensive e-mail.

Sending e-Mails
If sending e-mails containing personal, confidential, classified or financially sensitive data to external third parties or agencies, refer to the Section e-mailing Personal, Sensitive, Confidential or Classified Information.

E-mailing Personal, Sensitive, Confidential or Classified Information
Assess whether the information can be transmitted by other secure means before using e-mail.
The use of Hotmail, Gmail, AOL or any other Internet based webmail service for sending e-mail containing sensitive information is not permitted.

Where your conclusion is that e-mail must be used to transmit such data:

- Obtain express consent from your manager to provide the information by e-mail
- Exercise caution when sending the e-mail and always follow these checks before releasing the e-mail:
- Verify the details, including accurate e-mail address, of any intended recipient of the information
- Verify (by phoning) the details of a requestor before responding to e- mail requests for information
- Do not copy or forward the e-mail to any more recipients than is absolutely necessary
- Do not send the information to anyone whose details you have been unable to separately verify (usually by phone)
- Send the information with password protection
- Do not identify such information in the subject line of any e-mail
- Request confirmation of safe receipt

Roles and Responsibilities
The named E-Safety co-ordinator in this school is the Headteacher who has been designated this role as a member of the senior leadership team.

E-Safety in the Curriculum
ICT and online resources are increasingly used across the curriculum. We believe it is essential for E-Safety guidance to be given to the children on a regular and meaningful basis. E-Safety is embedded within our curriculum and we continually look for new opportunities to promote E-Safety.

- The school has a framework for teaching internet skills in ICT lessons.

- The school provides opportunities within a range of curriculum areas to teach about E-Safety

- Educating children on the dangers of technologies that maybe encountered outside school is done informally when opportunities arise and as part of the E-Safety curriculum

- Children are aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying. Children are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Childline or CEOP report abuse button

- Children are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the computing curriculum

Misuse and Infringements
Complaints
Complaints and/ or issues relating to E-Safety should be made to the Headteacher. Incidents should be logged and where necessary referred to the relevant agency in accordance with personnel or safeguarding procedures.

Inappropriate Material
All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the E-Safety co-ordinator.
Deliberate access to inappropriate materials by any user will lead to the incident being logged by the E-Safety co-ordinator, depending on the seriousness of the offence; investigation by the Headteacher/ LA, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences.

Internet Access
All use of is logged and regularly monitored. Whenever any inappropriate use is detected it will be followed up.

Parental Involvement
We believe that it is essential for parents/ carers to be fully involved with promoting E-Safety both in and outside of school and also to be aware of their responsibilities. We regularly communicate matters of E-Safety with parents/ carers and seek to promote a wide understanding of the benefits related to ICT and associated risks, through newsletters and workshops.
Parents/ carers are required to make a decision as to whether they consent to images of their child being taken/ used in the public domain (e.g., on school website).

Passwords and Password Security Guidance:
- ✓ Always use your own personal passwords to access computer based services
- ✓ Make sure you enter your personal passwords each time you logon
- ✓ Do not include passwords in any automated logon procedures
- ✓ Staff should change temporary passwords at first logon

- ✓ Change passwords whenever there is any indication of possible system or password compromise
- ✓ Do not record passwords or encryption keys on paper or in an unprotected file
- ✓ Only disclose your personal password to authorised ICT support staff when necessary, and never to anyone else
- ✓ Ensure that all personal passwords that have been disclosed are changed once the requirement is finished
- ✓ Passwords should contain a minimum of six characters and be difficult to guess

Protecting Personal, Sensitive, Confidential and Classified Information.

All staff are instructed to:

- Ensure that any school information accessed from own PC or removable media equipment is kept secure
- Ensure screens are locked before moving away from class computers during normal working day to prevent unauthorised access
- Ensure the accuracy of any personal, sensitive, confidential and classified information disclosed or shared with others
- Ensure that personal, sensitive, confidential or classified information is not disclosed to any unauthorised person
- Ensure the security of any personal, sensitive, confidential and classified information contained in documents you copy, scan or print. This is particularly important when shared copiers (multi-function print, scan and copiers) are used and when access is from a non-school environment
- Only download personal data from systems if expressly authorised to do so by your manager
- Not post any personal, sensitive, confidential, or classified information, or disseminate such information in any way that may compromise its intended restricted audience
- Keep screen displays out of direct view of any third parties when accessing personal, sensitive, confidential or classified information
- Ensure hard copies of data are securely stored and disposed of after use in accordance with the document labelling
- Only use equipment with an appropriate level of security for remote access
- To prevent unauthorised access to school systems, keep all access information such as telephone numbers, logon IDs and PINs confidential and do not disclose them to anyone
- Select PINs to ensure that they are not easily guessed, e.g. do not use your house or telephone number or choose consecutive or repeated numbers
- Avoid writing down or otherwise recording any network access information. Any such information that is written down must be kept in a secure place and disguised so that no other person will be able to identify what it is

- Protect School information and data at all times, including any printed material produced while using the remote access facility. Take particular care when access is from a non-school environment

School ICT Equipment
As a user of ICT, you are responsible for any activity undertaken on the school's ICT equipment provided to you.

- ✓ Do not allow your visitors to plug their ICT hardware into the school network points (unless special provision has been made).
- ✓ Ensure that all ICT equipment that you use is kept physically secure.
- ✓ 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. You are responsible for the backup and restoration of any of your data that is not held on the school's network drive
- ✓ It is recommended that a time locking screensaver is applied to all machines. Any PCs etc accessing personal data must have a locking screensaver as must any user profiles

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, parent/ carer, fellow professional or other 'client' using their personal device.

- ✓ Some children are allowed to bring personal mobile devices/phones by prior agreement and must be left in the school office.
- ✓ Visitors to EYFS will be asked to leave their phones in the school office.

Servers
Newly installed servers holding personal data are encrypted, therefore password protecting data.

- ✓ Servers are kept in a locked and secure environment
- ✓ Access rights are limited
- ✓ Servers are password protected and locked the server
- ✓ Existing servers have security software installed appropriate to the machine's specification
- ✓ Data is backed up regularly

Reviewed: October 2019
Next Review: October 2020

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 the Headteacher.

- ✓ I will only use the school's email / Internet / Intranet and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Board
- ✓ 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 children, staff and parents / clients are compatible with my professional role
- ✓ I will not give out my own personal details, such as mobile phone number and personal e- mail address, to children or other 'client'
- ✓ 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 Board. Personal or sensitive data taken off site must be encrypted
- ✓ I will not install any hardware of software without permission of the ICT Technician
- ✓ I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory
- ✓ Images of children 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 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 my professional role into disrepute
- ✓ I will support and promote the school's e-Safety and Data Security policies and help children to be safe and responsible in their use of ICT and related technologies
- ✓ I understand this forms part of the terms and conditions set out in my contract of employment (where appropriate)

User Signature

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

Signature : ***Date :***

Full Name : ***Job Title :***

Reviewed: October 2019
Next Review: October 2020