All Saints' Church of England Primary School

ACCEPTABLE USE OF ICT

"Loving to Learn, learning to Love"

"A new command I give you, Love one another.

As I have loved you, so you must love one another."

John 13:34

Ratified by Full Board of Governors: 09.11.2021 Review date: Autumn 2022

Policy Contents

1. INTRODUCTION

This policy outlines our purpose in providing ICT (Information and Communication Technology) facilities and equipment at All Saints' CE (Aided) Primary School and explains how the school is seeking to avoid the potential problems that unrestricted access to ICT facilities could give rise to. The school recognises that Information and Communication Technology changes and develops rapidly, and that it would be difficult for any policy to cover all situations that may present themselves even in the next few months. This policy should be used alongside other school policies. It is expected that every member of All Saints School, which includes parents and carers, will act at all times in a responsible, safe and professional way, and will at all times take into account the effect of their actions on any other member of the school.

2. GENERAL USE

2.1 The primary use of the school computing systems are for teaching and learning. A degree of personal use is permitted outside of core working hours or during lunch breaks. Users are personally responsible for exercising good judgement regarding the reasonableness and extent of personal use on the school computing system. Users should be guided by this policy to ensure they understand the appropriate use of the system, and if there is any uncertainty, users should consult their IT Manager/ Technician to gain clarification.

3. MONITORING

3.1 Monitoring of networks, systems, removable media, removable devices and data as well as online services which may include personal use such as social media, webmail and personal backing is undertaken for the purpose of confirming security, network and system performance and also staff usage.

3.2 The monitoring system we use it NetSupport DNA and it is also used to safeguard our system and to provide remote support for staff. Containing 1000+ key phases the system is constantly running to ensure that anything being searched or typed that is not appropriate for work is recorded either by a text file or a screenshot.

3.2.1 Every member of staff that has access to an All Saints' laptop is monitored under this system.

4. SECURITY AND PROPRIETARY INFORMATION

4.1 Users may not acquire, disclose or otherwise process School data for personal use or gain.

4.2 Any School data that the user may possess during their engagement with the School must be destroyed at the end of the contract, employment or engagement with the School.

4.3 Users must keep passwords secure and must not share logon accounts. Users are responsible for the security of their own accounts and passwords. No system or application passwords should be disclosed at any time to other users or support personal. Should the IT Manager/Technician require access to a user account, they will reset the password with the user's permission. Once complete, the password will again be reset allowing the user to replace it with one of their choice.

4.4 All laptops and workstations will be secured with a password-protected screensaver with the automatic activation feature set at 30 minutes.

4.5 While powered on, users must not leave their workstation or laptop unattended without locking the windows session to prevent unauthorised access. We suggest that you do this by either going to the windows menu and locking the computer or by clicking the 'Windows key + L' on the keyboard.

4.6 Users must use extreme caution when opening e-mail attachments received from unknown senders, as they may contain viruses or other malicious code.

4.7 Use and access to School systems and data stored is privileged, and must not be shared externally.

5. COPYRIGHT

5.1 Under the new General Data Protection Regulation (GDPR) Unauthorised copying of copyrighted material including, but not limited to, digitisation and distribution of photographs from magazines, logos or trade marks, books or other copyrighted sources, copyrighted music, video and the installation of any copyrighted software for which the School or the end user does not have an active license is strictly prohibited.

5.2 All users, including delegates, staff and students are reminded that School delivered courses and events are comprised of copyright materials and therefore should not be copied or distributed by any means without written permission of the school.

5.3 The school has a license which is provided by the Department for Education and allows the school to show copyright material but not hold or copy it to our systems.

6. COMPUTER EQUIPMENT USAGE

6.1 Overview

This section outlines the School policy relating to the use of computing equipment. The provision and use of school desktops, laptops or other computing devices is dependent on conformance with the rules outlined in this document and the policies within the school in its entirety.

6.2 Non-school Equipment

6.2.1 Non school equipment is define as equipment not owned and provided by the school, such as equipment belonging personally to any individual or third party school.

6.2.2 Non school desktops, laptops or any other peripheral device must not be connected to any school network or device without receipt of written permission from the IT Manager.

6.2.3 Connection of non school provided smart phones (of any manufacture or operating system) to a school desktop or laptop for the purposes of transferring or synchronising data is prohibited.

7. VISITOR ACCESS

7.1 Visitors to school premises are not permitted to connect any IT equipment to the school corporate network - this includes wired or wireless.

7.2 Should a visitor require internet access this should be notified to the IT Manager prior to their visit so 6 that appropriate steps can be put in place to accommodate for this.

7.3 Any visitor who is leading a presentation should either email the document in to the main Office or notify the school that they are bringing a USB stick in so that this can be check prior to use in the system.

7.4 All visitors must also comply with the Mobile Phone Policy and all mobile phones should be turned off and not brought out whilst in and around the school site.

8. UNACCEPTABLE USER AGREEMENT

8.1 Use of the school's computing facilities are subject to the user's acceptance of this policy. Misuse of these facilities will be considered a breach of School Policy and may result in disciplinary action or summary dismissal.

8.2 School IT systems must not be used to download, disseminate, send, receive, store, distribute, transmit, post, upload or display material that could be considered to be or contain material that is inappropriate. Any action in doing so will lead to disciplinary or legal action being taken by the school and may also constitute a criminal offence.

8.3 Inappropriate material includes, but is not limited to:

- Child Abuse
- Pornography
- Racism
- Defamation
- Torture
- Bestiality
- Sexism
- Violence
- Rape
- Other illegal, immoral or indecent material
- Gambling Sites

8.4 Should a user receive any suspect material, regardless of source, or become aware of any location of such material, the incident must be reported immediately to the IT Manager. If a user has been inadvertently exposed to prohibited material in any way, they should contact the school HR department who will be able to provide additional support and advice.

8.5 Users are personally responsible for exercising good judgement regarding the reasonableness and extent of personal use of School IT facilities. Users should be guided by the policies detailed within this document to ensure their use is appropriate, and if there is any uncertainty, users should consult their manager, instructor or the IT Manager to gain clarification.

8.6 School IT services are provided for school business use and must not be used for personal financial gain.

8.7 Staff may not use the services for, or in connection with, any third party business interest.

8.8 Any misuse of IT computing systems involving criminal activities may result in summary dismissal and/ or the user being reported to the relevant authorities.

8.9 Where any delegate or student is found to have breached any policy rile within this document, the incident will be report to their manager.

8.10 Please be aware that all unacceptable use of any school ICT equipment will also appear on the 7 NetSupport monitoring system. For further information on the monitoring software please see point 3.

8.11 Any apps that wish to be used on staff or student iPads must been requested through the IT manager. The school is required to ensure that everything that staff or students have access to are relevant and appropriate for the designated age groups. Should you have any questions regarding this please speak with the IT manager.

9. SCHOOL ASSET REGISTER

9.1 All ICT equipment that has been purchased by the school will appear on the schools Asset Register.

9.2 Every item is tagged with an All Saints' Asset Tag and has been inputted into the register. The register holds all of the information regarding the use, location, member assigned, cost, replacement cost, purchase date, warranty information, serial numbers, supplier, update/check information and general notes. All of this is held on the asset register until it has reached end of life and the product is removed from use.

9.3 Any items that are removed from the asset register have to be authorised via the Resource Management Committee. Items will only be removed should they be unusable or not safe.

10. STAFF ACCEPTABLE USER AGREEMENT

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 and personal use. This agreement is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT in school or at home. All staff are expected to sign this policy and adhere at all times to its contents. I understand that I must use the School ICT systems and equipment in a responsible way, to minimise the risk to my safety, to the safety and security of the ICT systems, other users and to comply with securing data under the School's Data Protection policy.

For my professional and personal safety:

- I understand that if I setup my work email on my own personal device i.e. mobile phone, iPad/laptop I must use a secure access code that auto locks after 30 secs and does not display messages on the locked screen to protect the data to comply with data protection legislation.
- 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 Head teacher;
- I understand that this agreement also applies to the use of School ICT systems out of school (e.g. laptops, emails);
- I understand the school ICT systems are intended for work use only and will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head.
- I will keep my usernames and passwords private and not disclose any passwords provided to me by the school or other related authorities.
- I will not use anyone's else username and password without the explicit permission of either the Head teacher.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute. This includes any private social networking sites / blogs etc. that I create or actively contribute to;
- I will ensure I regularly update any account of social networking sites / blogs etc. that I create or actively contribute to be set at the maximum settings. If needed, I will seek advice from the school's ICT team should I require support.
- I will not use chat or social networking sites nor will I access my personal emails whilst on the school premises.
- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is

deemed necessary that I am required by law to disclose such information to an appropriate authority;

- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the appropriate line manager / school named contact or use the Whistle Blowing Policy.
- 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.
- Accept responsibility for any hardware such as laptops and iPads provided for me by the school. I will ensure that the school hardware is only used to support my professional responsibilities and that I will notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- I will only use the approved, secure e-mail system for any school business;
- I will ensure that I do not use USB sticks or other external memory saving devices that put me at risk of losing sensitive information. Instead I will use the schools secure cloud based system and online portal to gain remote access to the network;
- I will not install any hardware of software without permission of Head.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.

Professional communication and actions when using School ICT systems:

- I will communicate with others in a professional manner;
- I will ensure when emailing information of a sensitive nature regarding the name of either a pupil or a member of staff I will use initials only within the context of that communication
- I will ensure that all electronic communications with pupils, parents and staff are compatible with my professional role;
- I will not give out my own personal details, such as mobile phone number, personal blog/e-mail address and social networking identities to pupils; or parents whose children attend the School. (this includes former pupils and parents).
- I will not have pupils, or parents whose children attend the School (this includes former pupils and parents) as friends on my social networking site.
- 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 individual involved. Images of pupils must not be taken by personal digital cameras or camera phones. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Head teacher.
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing any viruses or other harmful programmes.
- I will ensure that I report any breach of data to the appropriate person within the School.

I have read and understood the Acceptable Use of ICT Policy, and I agree to abide by the Rules for Acceptable Use of ICT given above.

Signature:…… Date……..

Full Name:…….. (Printed)

Job title:……..

11. EYFS STUDENT ACCEPTABLE USER AGREEMENT

Dos and Don’ts of ICT

Do:

- Only go on things that the teacher has told me to go on
- Hold the school iPads with two hands or put them down on the table
- Make sure I don’t have any water or drinks bottles near the ICT equipment
- If you see something that doesn't look right, turn your iPad over/close the lid of the laptop, put your hand up and tell a teacher
- Always listen to the teachers instruction before using the equipment

Don’ts:

- Don’t run whilst holding any ICT equipment
- Don’t go on anything that you haven't been told to
- Don’t mess around whilst the equipment whilst the teacher is talking
- Don’t take any photos or videos on the iPads unless told to by the teacher

Please note that internet and email use may be subject to monitoring

Useful websites:

CEOP is a part of the UK police force dedicated to the prevention of child sexual abuse. There is an excellent educational programme, as well as advice and videos for all ages on their website. - www.ceop.gov.uk

IWF (Internet Watch Foundation) provides the UK hotline to report criminal online content. - www.iwf.org.uk

Think U Know provides useful information for children of all ages and parents too. www.thinkuknow.co.uk

Kidsmart is an award-winning internet safety programme for children. www.kidsmart.org.uk

Bullying Uk provides information and advice about bullying for children, parents and schools. www.bullying.co.uk

NSPCC online safety section provide tips on how to keep children safe online. www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety

The Digizen website provides information for educators, parents, carers, and young people. It is used to strengthen their awareness and understanding of what digital citizenship is and encourages users of technology to be and become responsible digital citizens. www.digizen.org

Parents will be requested to sign a declaration to confirm that they have read this policy and explained it to their child/children, and also to confirm they have made their child/children aware that use of internet and email in school may be monitored. (See appendix attached)

Acceptable Use Policy (EYFS Pupils) 2021

I have read the above Acceptable Use Policy and explained it to my child/children. I have also made my child/children aware that the use of internet and email in school may be monitored.

Signed:…… Date:……

Printed:……

Parent/Carer of:……

Class:…….

12. KS1 STUDENT ACCEPTABLE USER AGREEMENT

The use of ICT within schools has enormous benefits to education, however there are reasons why the school and the local authority must put some restrictions in place, such as: ICT equipment is very expensive to buy and maintain; the school and the local authority have a duty of care to ensure that you are safe and that you are not exposed to illegal or unsuitable content. It is hoped that these restrictions do not interfere with your education, but if you feel otherwise you are encouraged to talk to a member of staff to discuss any issues.

Please note that internet and email use may be subject to monitoring.

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers / tablets.
- I will only use activities that a teacher or suitable adult has told or allowed me to use.
- I will take care of the computer and other equipment.
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong.
- I will tell a teacher or suitable adult if I see something that upsets me on the screen.
- I know that if I make the wrong choices, I might not be allowed to use a computer / tablet.

Don't forget, it is never too late to tell someone if something or someone makes you feel uncomfortable.

Useful websites:

CEOP is a part of the UK police force dedicated to the prevention of child sexual abuse. There is an excellent educational programme, as well as advice and videos for all ages on their website. - www.ceop.gov.uk

IWF (Internet Watch Foundation) provides the UK hotline to report criminal online content. - www.iwf.org.uk

Think U Know provides useful information for children of all ages and parents too. www.thinkuknow.co.uk

Kidsmart is an award-winning internet safety programme for children. www.kidsmart.org.uk

Bullying Uk provides information and advice about bullying for children, parents and schools. www.bullying.co.uk

NSPCC online safety section provide tips on how to keep children safe online. www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety

The Digizen website provides information for educators, parents, carers, and young people. It is used to strengthen their awareness and understanding of what digital citizenship is and encourages users of technology to be and become responsible digital citizens.
www.digizen.org

Parents will be requested to sign a declaration to confirm that they have read this policy and explained it to their child/children, and also to confirm they have made their child/children aware that use of internet and email in school may be monitored. (See appendix attached)

Acceptable Use Policy (Key Stage 1 Pupils) 2021

I have read the above Acceptable Use Policy and explained it to my child/children. I have also made my child/children aware that the use of internet and email in school may be monitored.

Signed:…… Date:……

Printed:……

Parent/Carer of:……

Class:…….

13. KS2 STUDENT ACCEPTABLE USER AGREEMENT

The use of ICT within schools has enormous benefits to education, however there are reasons why the school and the local authority must put some restrictions in place, such as: ICT equipment is very expensive to buy and maintain; the school and the local authority have a duty of care to ensure that you are safe and that you are not exposed to illegal or unsuitable content. It is hoped that these restrictions do not interfere with your education, but if you feel otherwise you are encouraged to talk to a member of staff to discuss any issues.

Please note that internet and email use may be subject to monitoring.

Use of the Internet - the internet is provided to help you with learning activities such as research, online activities, online educational games and many other things. The internet is not to be used to access anything which is illegal, or anything that someone else may find offensive. If you are unsure, or if you come across anything you feel is unsuitable, you should turn your computer monitor off and let your teacher/teaching assistant know. Never try to bypass the security, these are all monitored.

User Areas - your user area is provided for you to save school work. It is not to be used to save music or other files that you have brought in from home.

Social Networking – the use of such sites will not be allowed in our school. If access is allowed to social networking (for example Bebo, Facebook, Flickr) at home you should never upload pictures or videos of others without their permission. You should also be aware of any age restrictions relating to such sites (many social networking sites have a minimum age of 13 years). It is not advisable to upload pictures or videos of yourself - videos and pictures can easily be copied, changed and used against you without you knowing. You should never make negative or bad remarks about the school or anyone within the school. Always keep your personal information private to invited friends only and never post personal information such as your full name, date of birth, address, school, phone number etc. Consider using a nickname and only inviting people you know. Universities and future employers have been known to search social networking sites.

Beware of fake profiles and people pretending to be somebody else. If something doesn't feel right, follow your instincts and report it to an appropriate adult.

Some social networking sites have a chat facility. You should never chat to anyone that you don't know or don't recognise. It is recommended that you never meet a stranger after meeting them online. If you do, always inform your parents and take one of them with you.

Security - you should never try to bypass any of the security in place. This security is in place to protect you from illegal sites, and to stop others from hacking into other people's accounts. Security on the school computers is monitored.

Copyright - you should never take information from the internet and use it as your own. A lot of information is copyright, which means that it is owned by somebody else and it is illegal to use this information without permission from the owner. If you are unsure, ask your teacher.

Etiquette - Always be polite and don't swear. Consider what you are saying, and how it might be read by somebody else. Without emotions it is difficult to show emotions in things like emails and blogs, and some things you write may be read incorrectly.

Mobile Phones - Most modern mobile phones offer the same services as a computer, i.e. Facebook, YouTube, email access etc. This can be a great way of keeping in touch with your friends and family. But, in the same way that some internet services can be used inappropriately, the same is true with mobile phones. Mobile Phones are not allowed in our school unless under very special circumstances, and only with the permission of the Head Teacher. Never take inappropriate pictures of yourself and send to your friends or upload onto social networking sites. Never forward inappropriate pictures that you have received from somebody else. In some circumstances this can be an illegal act.

Useful websites:

CEOP is a part of the UK police force dedicated to the prevention of child sexual abuse. There is an excellent educational programme, as well as advice and videos for all ages on their website. - www.ceop.gov.uk

IWF (Internet Watch Foundation) provides the UK hotline to report criminal online content. - www.iwf.org.uk

Think U Know provides useful information for children of all ages and parents too. www.thinkuknow.co.uk

Kidsmart is an award-winning internet safety programme for children. www.kidsmart.org.uk

Bullying Uk provides information and advice about bullying for children, parents and schools. www.bullying.co.uk

NSPCC online safety section provide tips on how to keep children safe online. www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety

The Digizen website provides information for educators, parents, carers, and young people. It is used to strengthen their awareness and understanding of what digital citizenship is and encourages users of technology to be and become responsible digital citizens. www.digizen.org

E Safety (do's and don'ts)

Some simple do's and don'ts for everybody (courtesy of CEOP):

- Never give out personal details to online friends that you don't know offline. Understand what information is personal: i.e. email address, mobile number, school name, sports club, meeting up arrangements, pictures or videos of yourself, friends or family. Small pieces of information can easily be pieced together to form a broad insight into your personal life and daily activities.
- Think carefully about the information and pictures you post on your profiles. Once published online, anyone can change or share these images.
- It can be easy to forget that the internet is not a private space, and as result sometimes people engage in risky behaviour online. Don't post any pictures, videos or information on your profiles, or in chat rooms, that you would not want a parent or carer to see.
- If you receive spam or junk emails and texts, never believe the content, reply to them or use them. Don't open files that are from people you don't know. You won't know what they contain—it could be a virus, or worse - an inappropriate image or film.
- Understand that some people lie online and that it's better to keep online 'mates' online. Never meet up with any strangers without an adult that you trust.

Don't forget, it is never too late to tell someone if something or someone makes you feel uncomfortable.

Parents will be requested to sign a declaration to confirm that they have read this policy and explained it to their child/children, and also to confirm they have made their child/children aware that use of internet and email in school may be monitored. (See appendix attached)

Acceptable Use Policy (Key Stage 2 Pupils) 2021

I have read the above Acceptable Use Policy and explained it to my child/children. I have also made my child/children aware that the use of internet and email in school may be monitored.

Signed:…… Date:……

Printed:……

Parent/Carer of:……

Class:…….

14. LETTER HOME TO PARENTS

Dear Parents/Carers,

Acceptable Use of ICT

Our school is equipped with computers, which allow children to have supervised access to educational software, to school email and to the internet. In addition, the school has other equipment, such as scanners, digital cameras, camcorders and digital projectors, which can be linked to computers. These allow teachers to record pupils' work, for example in drama, dance and art, and allow pupils to create and show their own presentations and films. Together, this equipment is called ICT (Information and Communication Technology) equipment.

The school is aware that there have been widely publicised concerns about pupils having access to undesirable materials when they use the internet. We believe that the educational advantages of enabling the children supervised access to the internet greatly outweigh the likely problems if appropriate safeguards are put in place. We have purchased our internet access from E2BN, an educational supplier that operates a filtering system to block access to inappropriate materials. Our computer screens are in public view and, as stated above, internet access will be supervised.

The school has prepared a detailed policy covering acceptable use of ICT in school; this is intended to help us make the most of the opportunities that ICT offers whilst minimising the possible risks. It includes a set of Rules for Responsible ICT Use that we will be teaching the children and I attach a copy of these. I have a number of leaflets from national bodies that explain the issues further and some of these also cover internet use by children at home.

We regret that, because it is not possible to be certain of the originator of an email message, the school is unable to accept an email as parental authorisation of a pupil absence.

Should you wish to read our school Acceptable Use of ICT Policy or to discuss any aspect of internet use please telephone me to arrange an appointment. A copy of the policy is available on the school website at www.allsaints.peterborough.sch.uk

Yours sincerely,

Mr D Roberts

Acting Head Teacher