ICT and Internet Acceptable Use Policy

Date: July 2022
Review date: July 2026
Approved by the Advisory Board: July 2022

Linked with other policies:

- Safeguarding incorporating Child Protection
- Behaviour
- Disciplinary
- Data protection
- Privacy Notice
- Workforce Privacy Notice
- Cyberbullying
- Staff Code of Conduct
- Internet, Social Media and Email Use

Signed: 

Version Control

Version	Date of review/change(s)	Page and paragraphs affected	Summary of update
1	July 2021	Page3 paragraph 4 Page 6 section 5.2.1 Page 6 section 5.4 Page 6 section 6 Page 8 section 8.5 Page 8 section 9 Page 9 paragraph 6 Page 9 section 10 Page 9 Page 10 Appendix 1 Page 17 Page 19	See appendix 5 ICT Acceptable use agreement for Directors, Volunteers and Visitors. Signed copies for volunteers and visitors are kept for 12 months in a locked filing cabinet in the office. Addition of further social media platforms Removal of the word define Change of how parents/carers give permission for their child to access the internet. Deletion of 2nd paragraph and replaced with 'All personal devices including USB memory sticks and encrypted USB memory sticks are banned from All Saints School.' Change to staff positions and remove Netcentral Solutions Ltd. Change Smoothwall to Securly Policy review changed to annually Removal of section 11 'Related policies' – see front cover. Change 'Facebook' to 'Social Media' Addition of appendix 6 – Laptop Policy and Agreement Addition of appendix 7 – Student IT Equipment Loan Agreement
2	July 2022	P5	school's IT Manager (external support from Netcentral
		P5	contact the school ICT Manager or the school Director.

1. Introduction and aims

ICT is an integral part of the way our school works, and is a critical resource for students, staff, Directors, volunteers and visitors. It supports teaching and learning, and the pastoral and administrative functions of the school.

However, the ICT resources and facilities our school uses also pose risks to data protection, online safety and safeguarding.

This policy aims to:

- Set guidelines and rules on the use of school ICT resources for staff, students, parents, visitors, volunteers, contractors and Directors
- Establish clear expectations for the way all members of the school community engage with each other online and the outside world
- Support the school's policy on data protection, online safety and safeguarding
- Prevent disruption to the school through the misuse, or attempted misuse, of ICT systems
- Support the school in teaching students safe and effective internet and ICT use.

This policy covers all users of our school's ICT facilities, including Directors, staff, students, volunteers, contractors and visitors. See appendix 5 ICT Acceptable use agreement for Directors, Volunteers and Visitors. Signed copies for volunteers and visitors are kept for 12 months in a locked filing cabinet in the office. Breaches of this policy may be dealt with under the most appropriate policy for example, GDPR policy, Staff/Student Code of Conduct

2. Relevant legislation and guidance

This policy refers to, and complies with, the following legislation and guidance:

- Data Protection Act
- Human Rights Act
- Education Act
- Freedom of Information Act
- Independent School Standards
- Keeping Children Safe in Education
- Searching, screening and confiscation: advice for schools

3. Definitions

- **"ICT facilities":** includes all facilities, systems and services including, but not limited to, network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, and any device system or service which may become available in the future which is provided as part of the ICT service
- **"Users":** anyone authorised by the school to use the ICT facilities, including Directors, staff, students, volunteers, contractors and visitors
- **"Personal use":** any use or activity not directly related to the user's employment, study or purpose
- **"Authorised personnel":** employees/contractors authorised by the school to perform systems administration and/or monitoring of the ICT facilities
- **"Materials":** files and data created using the ICT facilities including, but not limited to, documents, photos, audio, video, printed output, web pages, social networking sites, and blogs

4. Unacceptable use

The following is considered unacceptable use of the school's ICT facilities by any member of the school community. Any breach of this policy may result in disciplinary or behaviour proceedings (see section 4.2 below).

Unacceptable use of the school's ICT facilities includes:

- Using the school's ICT facilities to breach intellectual property rights or copyright;
- Using the school's ICT facilities to bully or harass someone else, or to promote unlawful discrimination;
- Breaching the school's policies or procedures;
- Any illegal conduct, or statements which are deemed to be advocating illegal activity;
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate;
- Activity which defames or disparages the school, or risks bringing the school into disrepute;
- Sharing confidential information about the school, its students, or other members of the school community;
- Connecting any device to the school's ICT network without approval from authorised personnel;
- Setting up any software, applications or web services on the school's network without approval by authorised personnel, or creating or using any program, tool or item of software designed to interfere with the functioning of the ICT facilities, accounts or data;
- Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel;
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities;
- Causing intentional damage to ICT facilities;
- Removing, deleting or disposing of ICT equipment, systems, programs or information without permission by authorised personnel;
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation;
- Using inappropriate or offensive language;
- Promoting a private business, unless that business is directly related to the school;
- Using websites or mechanisms to bypass the school's filtering mechanisms.

This is not an exhaustive list. The school reserves the right to amend this list at any time. The Headteacher or Directors will use professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the school's ICT facilities.

4.1 Exceptions from unacceptable use

Where the use of school ICT facilities is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the Headteacher's discretion through agreement with the Directors.

4.2 Sanctions

Students and staff who engage in any of the unacceptable activity listed above may face disciplinary action in line with the school's policies on staff discipline and Staff/Student Code of Conduct.

5. Staff (including Directors, volunteers, and contractors)

5.1 Access to school ICT facilities and materials

The school's network is managed by the school's IT Manager (external support from Netcentral Solutions Ltd) who manages access to the school's ICT facilities and materials for school staff. That includes, but is not limited to:

- Computers, tablets and other devices
- Access permissions for certain programmes or files on direction from the Headteacher

Staff will be provided with unique log-in/account information and passwords that they must use when accessing the school's ICT facilities. These passwords should never be shared.
Staff who have access to files they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the school ICT Manager or the school Director.

5.1.1 Use of phones and email

The school provides each member of staff with an email address.
This email account should be used for work purposes only.
All work-related business must be conducted using the email address the school has provided.
Staff must not share their personal email addresses with parents and students, and must not send any work-related materials using their personal email account.
Staff must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.
Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents. Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.
Staff must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient.
If staff receive an email in error, the sender should be informed and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.
If staff send an email in error which contains the personal information of another person, they must inform the Headteacher or school support manager and the Data Protection Officer immediately and follow our data breach procedure.
Staff must not give their personal phone numbers to parents or students. Staff must use phones provided by the school to conduct all work-related business.
School phones must not be used for personal matters.
Staff who are provided with mobile phones as equipment for their role must abide by the same rules for ICT acceptable use as set out in section 4.

5.1.2 All staff receiving a school device must sign and agree with the Staff Laptop Usage Policy and Agreement (see Appendix 6).

5.2 Personal use

Staff are not permitted to use school ICT facilities for personal use unless permission has been granted from the Headteacher.

Staff may not use the school's ICT facilities to store personal, non-work-related information or materials (such as music, videos, or photos).

Staff should be aware that use of the school's ICT facilities for personal use may put personal communications within the scope of the school's ICT monitoring activities (see section 5.5). Where breaches of this policy are found, disciplinary action may be taken.
Staff should take care to follow the school's guidelines on social media (see Appendix 1) and use of email (see section 5.1.1) to protect themselves online and avoid compromising their professional integrity.

5.2.1 Personal social media accounts
Members of staff should ensure that their use of social media, either for work or personal purposes, is appropriate at all times.
The school has guidelines for staff on appropriate security settings for social media accounts (Facebook, Twitter, Tik Tok, WhatsApp, etc) (see Appendix 1).

5.3 Remote access
We allow staff to access the school's ICT facilities and materials remotely. This is managed by Netcentral Solutions Ltd
Staff accessing the school's ICT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on-site. Staff must be particularly vigilant if they use the school's ICT facilities outside the school and take such precautions as Netcentral Solutions Ltd or the Headteacher may require from time to time against importing viruses or compromising system security.
Our ICT facilities contain information which is confidential and/or subject to data protection legislation. Such information must be treated with extreme care and in accordance with our data protection policy.
The school's data protection policy can be found on the school server or on the school website.

5.4 Monitoring of school network and use of ICT facilities
The school reserves the right to monitor the use of its ICT facilities and network. This includes, but is not limited to, monitoring of:

- Internet sites visited
- Bandwidth usage
- Email accounts
- Telephone calls
- User activity/access logs
- Any other electronic communications

Only authorised ICT staff may inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law.
The school monitors ICT use in order to:

- Obtain information related to school business
- Investigate compliance with school policies, procedures and standards
- Ensure effective school and ICT operation
- Conduct training or quality control exercises
- Prevent or detect crime
- Comply with a subject access request, Freedom of Information Act request, or any other legal obligation

6. Students

6.1 Access to ICT facilities

Computers and equipment are available to students with the agreement of the Code of Conduct. Any parent/carer wishing their child to use the internet at school must sign the Permission to Use the Internet and Technology section on the school's admission form, if not signed access is denied. Completed forms will be held in student files. Any student and parent receiving a school device must sign and agree to the Student IT Equipment Loan Agreement (see Appendix 7).

6.2 Search and deletion

Under the Education Act 2011, and in line with the Department for Education's guidance on searching, screening and confiscation, the school has the right to search students' phones, computers or other devices for pornographic images or any other data or items banned under school rules or legislation.
The school can, and will, delete files and data found on searched devices if we believe the data or file has been, or could be, used to disrupt teaching or break the school's rules.

6.3 Unacceptable use of ICT and the internet outside of school

The school will sanction students, in line with the Behaviour Policy, if a student engages in any of the following **at any time** (even if they are not on school premises):

- Using ICT or the internet to breach intellectual property rights or copyright
- Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, other students, or other members of the school community
- Gaining or attempting to gain access to restricted areas of the network, or to any password protected information, without approval from authorised personnel
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities
- Causing intentional damage to ICT facilities or materials
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation
- Using inappropriate or offensive language

7. Parents

7.1 Access to ICT facilities and materials

Parents do not have access to the school's ICT facilities as a matter of course.
However, parents working for, or with, the school in an official capacity (for instance, as a volunteer or as a member of FRIENDS of All Saints) may be granted an appropriate level of access, or be permitted to use the school's facilities at the Headteacher's discretion.
Where parents are granted access in this way, they must abide by this policy as it applies to staff.

7.2 Communicating with or about the school online

We believe it is important to model for students, and help them learn, how to communicate respectfully with, and about, others online.
Parents play a vital role in helping model this behaviour for their children, especially when communicating with the school through our website and social media channels.
We ask parents to sign the agreement in Appendix 2.

8. Data security

The school takes steps to protect the security of its computing resources, data and user accounts. However, the school cannot guarantee security. Staff, students, parents and others who use the school's ICT facilities should use safe computing practices at all times.

8.1 Passwords

All users of the school's ICT facilities should set strong passwords for their accounts and keep these passwords secure.

Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control.
Members of staff or students who disclose account or password information will face disciplinary action.
Parents or volunteers who disclose account or password information will have their access rights revoked.

8.2 Software updates, firewalls, and anti-virus software

All of the school's ICT devices that support software updates, security updates, and anti-virus products will be configured to perform such updates regularly or automatically.
Users must not circumvent or make any attempt to circumvent the administrative, physical and technical safeguards we implement and maintain to protect personal data and the school's ICT facilities.
Any personal devices using the school's network must all be configured in this way.

8.3 Data protection

All personal data must be processed and stored in line with data protection regulations and the school's data protection policy.
The data protection policy can be found on the school website.

8.4 Access to facilities and materials

All users of the school's ICT facilities will have clearly defined access rights to school systems, files and devices.
Students will only be allowed access after completing and signing the agreement in the Student Planner.
These access rights are managed by Netcentral Solutions Ltd.
Users should not access, or attempt to access, systems, files or devices to which they have not been granted access. If access is provided in error, or if something a user should not have access to is shared with them, they should alert the Headteacher immediately.
Users should always log out of systems and lock their equipment when they are not in use to avoid any unauthorised access. Equipment and systems should always be logged out of and closed down completely at the end of each working day.

8.5 Encryption

The school ensures that its devices and systems has a level of encryption.
All personal devices including USB memory sticks and encrypted USB memory sticks are banned from All Saints School.

9. Internet access

The school wireless internet connection is secured via WPA2 encryption.
The school's internet access, whether via wireless (Wi-Fi) or a cabled connection is filtered and secured by an on-premises Securly content filtering solution.
Any unauthenticated user or device will have the fully restricted 'Student' profile for internet access. Upon logging in to a computer, you are then authenticated as your user and therefore given a level of filtering that

is appropriate (ie. Student, Staff, Unrestricted). Reporting is in place which can and will log your internet usage including search history.
Encrypted (https://) websites are decrypted and therefore not hidden from the filtering.
Exclusions for encrypted sites are set to exclude certain sites such as Internet Banking.
The School's wireless network is presented as two Service Set Identifiers (SSIDs). These are two, segregated networks and have the following functions.

All Saints-Private This network is for use on all school owned/approved devices and allows a device to have filtered, secure access to the internet and the school's server.
The password for this wireless network is held by Netcentral Solutions Ltd and is not for circulation.

All Saints-Guest This network is for use on all non-school devices such as staff mobile phones. It is unable to access the school's server and may be subject to speed restrictions so as to not impair the main school network.
The password for this wireless network is available from the School office.

Website block and unblock requests can be reported to the Finance Director or IT Manager.

9.1 Students
Students should only access the internet via an approved school device, connected to the filtered **All Saints-Private** wireless network or via a cabled connection.

9.2 Parents and visitors
Parents and visitors to the school will not be permitted to use the school's Wi-Fi unless specific authorisation is granted by the Headteacher.
The Headteacher will only grant authorisation if:

- Parents are working with the school in an official capacity (e.g. as a volunteer or as a member of FRIENDS of All Saints)
- Visitors need to access the school's Wi-Fi in order to fulfil the purpose of their visit (for instance, to access materials stored on personal devices as part of a presentation or lesson plan)

Staff must not give the Wi-Fi password to anyone who is not authorised to have it. Doing so will result in disciplinary action.

10. Monitoring and review

The Headteacher and Directors monitor the implementation of this policy, including ensuring that it is updated to reflect the needs and circumstances of the school.
This policy will be reviewed annually.
The Advisory Board is responsible for approving this policy.

Appendix 1: Social Media cheat sheet for staff

Don't accept friend requests from students on social media

10 rules for school staff on Social Media

1. Change your display name – use your first and middle name, use a maiden name, or put your surname backwards instead.
2. Change your profile picture to something unidentifiable, or if not, ensure that the image is professional.
3. Check your privacy settings regularly.
4. Be careful about tagging other staff members in images or posts.
5. Don't share anything publicly that you wouldn't be just as happy showing your students.
6. Don't use social media sites during school hours.
7. Don't make comments about your job, your colleagues, our school or your students online – once it's out there, it's out there.
8. Don't associate yourself with the school on your profile (e.g. by setting it as your workplace, or by 'checking in' at a school event).
9. Don't link your work email address to your social media accounts. Anyone who has this address (or your personal email address/mobile number) is able to find you using this information.
10. Consider uninstalling the Facebook app from your phone. The app recognises Wi-Fi connections and makes friend suggestions based on who else uses the same Wi-Fi connection (such as parents or students).

Check your privacy settings

- Change the visibility of your posts and photos to **'Friends only'**, rather than 'Friends of friends'. Otherwise, students and their families may still be able to read your posts, see things you've shared and look at your pictures if they're friends with anybody on your contacts list.
- Don't forget to check your **old posts and photos** – go to bit.ly/2MdQXMN to find out how to limit the visibility of previous posts.
- The public may still be able to see posts you've **'liked'**, even if your profile settings are private, because this depends on the privacy settings of the original poster.
- **Google your name** to see what information about you is visible to the public.
- Prevent search engines from indexing your profile so that people can't **search for you by name** – go to bit.ly/2zMdVht to find out how to do this.
- Remember that **some information is always public**; your display name, profile picture, cover photo, user ID (in the URL for your profile), country, age range and gender.

What do to if…

A student adds you on social media

- In the first instance, ignore and delete the request. Block the student from viewing your profile
- Check your privacy settings again, and consider changing your display name or profile picture
- If the student asks you about the friend request in person, tell them that you're not allowed to accept friend requests from students and that if they persist, you'll have to notify senior leadership and/or their parents. If the student persists, take a screenshot of their request and any accompanying messages
- Notify the senior leadership team or the Headteacher about what's happening

A parent adds you on social media

It is at your discretion whether to respond. Bear in mind that:

- Responding to one parent's friend request or message might set an unwelcome precedent for both you and other teachers at the school
- Students may then have indirect access through their parent's account to anything you post, share, comment on or are tagged in

If you wish to decline the offer or ignore the message, consider drafting a stock response to let the parent know that you're doing so

You're being harassed on social media, or somebody is spreading something offensive about you

- **Do not** retaliate or respond in any way
- Save evidence of any abuse by taking screenshots and recording the time and date it occurred
- Report the material to Facebook or the relevant social network and ask them to remove it
- If the perpetrator is a current student or staff member, our mediation and disciplinary procedures are usually sufficient to deal with online incidents found in the Grievance Policy.
- If the perpetrator is a parent or other external adult, a senior member of staff should invite them to a meeting to address any reasonable concerns or complaints and/or request they remove the offending comments or material
- If the comments are racist, sexist, of a sexual nature or constitute a hate crime, you or a senior leader should consider contacting the police

Appendix 2: Acceptable use of the internet: agreement for parents and carers

Acceptable use of the internet: agreement for parents and carers	
Name of parent/carer: **Name of child:**	
Online channels are an important way for parents/carers to communicate with, or about, our school. The school uses the following channels: • Email/text groups for parents (for school announcements and information)	
When communicating with the school via official communication channels, or using private/independent channels to talk about the school, I will: • Be respectful towards members of staff, and the school, at all times • Be respectful of other parents/carers and children • Direct any complaints or concerns through the school's official channels, so they can be dealt with in line with the school's complaints procedure. I will not: • Use private groups, the school's Facebook page, or personal social media to complain about or criticise members of staff. This is not constructive and the school can't improve or address issues if they aren't raised in an appropriate way • Use private groups, the school's Facebook page, or personal social media to complain about, or try to resolve, a behaviour issue involving other students. I will contact the school and speak to the appropriate member of staff if I'm aware of a specific behaviour issue or incident • Upload or share photos or videos on social media of any child other than my own, unless I have the permission of other children's parents/carers.	
Signed:	**Date:**

Appendix 3: Acceptable use agreement for those student 12 year-old and above

Acceptable use of the school's ICT facilities and internet: agreement for students and parents/carers	
Name of student:	
When using the school's ICT facilities and accessing the internet in school, I will not: • Use them for a non-educational purpose • Use them without a teacher being present, or without a teacher's permission • Use them to break school rules • Access any inappropriate websites • Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity) • Use chat rooms • Open any attachments in emails, or follow any links in emails, without first checking with a teacher • Use any inappropriate language when communicating online, including in emails • Share my password with others or log in to the school's network using someone else's details • Bully other people I understand that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others. I will always use the school's ICT systems and internet responsibly. I understand that the school can discipline me if I go against what is set out in the Student Planner, even if I'm not in school when I do them at the time.	
Signed (student):	**Date:**
Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for students using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 4: Acceptable use agreement for those students 11 year old and younger

Acceptable use of the school's ICT facilities and internet: agreement for students and parents/carers	
Name of student:	
When I use the school's ICT facilities (like computers and equipment) and get on the internet in school, I will not: • Use them without asking a teacher first, or without a teacher in the room with me • Use them to break school rules • Go on any inappropriate websites • Go on Facebook or other social networking sites (unless my teacher said I could as part of a lesson) • Use chat rooms • Open any attachments in emails, or click any links in emails, without checking with a teacher first • Use mean or rude language when talking to other people online or in emails • Share my password with others or log in using someone else's name or password • Bully other people I understand that the school will check the websites I visit and how I use the school's computers and equipment. This is so that they can help keep me safe and make sure I'm following the rules. I will tell a teacher or a member of staff I know immediately if I find anything on a school computer or online that upsets me, or that I know is mean or wrong. I will always be responsible when I use the school's ICT systems and internet. I understand that the school can discipline me if I do go against what is set out in the Student Planner, even if I'm not in school when I do them at the time.	
Signed (student):	**Date:**
Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for students using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 5: ICT Acceptable use agreement for staff, directors, volunteers and visitors

Acceptable use of the school's ICT facilities and the internet: agreement for staff, Directors, volunteers and visitors	
Name of staff member/Director/volunteer/visitor:	
When using the school's ICT facilities and accessing the internet in school, or outside school on a work device, I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) • Use them in any way which could harm the school's reputation • Access social networking sites or chat rooms • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software, or connect unauthorised hardware or devices to the school's network • Share my password with others or log in to the school's network using someone else's details • Share confidential information about the school, its students or staff, or other members of the community • Access, modify or share data I'm not authorised to access, modify or share • Promote private businesses, unless that business is directly related to the school.	
I understand that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will let the designated safeguarding lead (DSL) know if a student informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's ICT systems and internet responsibly, and ensure that students in my care do so too.	
Signed (staff member/Director/volunteer/visitor):	**Date:**

Appendix 6: Laptop Usage and Policy Agreement

ALL SAINTS SCHOOL
School Road, Lessingham, Norwich, Norfolk
NR12 0DJ
01692 582083
www.allsaintslessingham.co.uk
E-mail: office@allsaintslessingham.co.uk

Directors: Mrs J Gardiner and Mrs R Smith

Laptop Usage Policy and Agreement

This policy outlines the responsibilities that staff must accept when they are issued a laptop. It applies to all members of staff who have been issued with a laptop, or the use of a laptop, from the school.
Any member of staff issued with a/with use of a laptop will need to confirm, by signing an acceptance of the policy, that he/she has read, understands and will comply with the policy. A copy of the policy will need to be signed by the member of staff, with a copy being retained in school until the laptop is returned or replaced.
When a member of staff is provided with a laptop, he/she accepts responsibility for safeguarding the laptop itself as well as the data stored on the laptop.
All laptops issued to staff will be checked by a person appointed by the Directors on a monthly basis to ensure proper use.

- I agree that the laptop at all times remains the property of All Saints School (Lessingham) Limited and that the laptop is provided for my use as a teacher to assist me in developing educational learning materials, assessment reporting and any other appropriate actions relevant to my position at All Saints School.
- I may use the laptop for the duration of my employment or until my role changes and I no longer require use of a laptop.
- I undertake to keep the laptop in good working order and to notify Rachel Smith or the Headteacher of any defect or malfunction of the laptop while in my care.
- I will not sell, assign, transfer or otherwise dispose of the laptop.
- I will not remove, conceal or alter any laptop package markings or tags or engrave or mark the laptop in any way that will reduce the value of the laptop.
- I will take due care of the laptop package at all times, including (but not limited to)
  - Ensure I have appropriate car and house insurance to be able to transport/use the laptop at home (the laptop is also covered under the insurance policy of All Saints School).
  - Not leaving the laptop unattended in a public place.
  - Not leaving the laptop unattended or unsecured in a classroom or other place in school.
  - Not leaving the laptop in plain view in an unattended or unsecured vehicle.
  - Not allowing the laptop to be accessed by any other person (unless authorised by All Saints School).
  - Not allowing the laptop to be interfered with, tampered with or altered by a third party.
  - Ensuring due care is taken in the handling, transporting and usage of the laptop.
  - Not using the laptop in environments that might increase the likelihood of damage.
- Any damage or loss must be reported to the Headteacher and Directors as soon as possible and the police in cases of theft.
- I will keep an independent record of the laptop serial number (included on this agreement) that I will use if need to report theft of the laptop to the police.

- I understand that I will not be held responsible for computer problems resulting from regular school-related use, but may be held responsible for any problems caused by my negligence as deemed by the Directors.
- I will not work on or save sensitive information (e.g. education records, personally identifiable information and confidential information) without taking proper precautions.
- I will never leave the laptop unattended and logged on. Always shut down, log off or lock the screen before walking away from the machine.
- I will upload all my files to the staff S: Drive to ensure no loss of data.
- I understand that the laptop has anti-virus software installed and I will keep this up to date and enabled.
- I will not open any email or attachment unless it is expected and from a legitimate source.
- I will report any security incidents (such as virus infections) to the Headteacher immediately in order to minimise the risk to the school.
- I will not download, install or use unauthorised software programmes. No personal programmes are to be used, e.g. iTunes.
- Any software that is required in addition to that provided with the laptop must first be approved by the Directors to ensure the correct permissions and licences are in place.
- I will make the laptop available on request of either the Directors or Headteacher for updates and any alterations to system setup.
- All members of staff are accountable for all network and systems access under their individual user ID. Passwords should be kept absolutely secret and should never be shared with anyone unless required by All Saints School for maintenance of the laptop.
- Laptops are provided for official use by authorised employees. All Saints School (Lessingham) Limited laptops must not be loaned or allowed to be used by others.
- I will comply with relevant laws, regulations and policies applying to the use of computers and information, e.g. licence, copyright, GDPR.
- All Saints School will not tolerate inappropriate materials such as pornographic, racist, defamatory or harassing files, photographs, videos or e-mail messages that might cause offence or embarrassment. Never store, use, copy or circulate such material on the laptop.

Failure to comply with this policy could lead to disciplinary action.

Items Loaned/Condition

Item	Loaned		Condition	
Laptop Computer	Yes	No	New	Used
Power Supply and Cord	Yes	No	New	Used
Mouse and USB	Yes	No	New	Used
Laptop Case	Yes	No	New	Used

Comments: (overall condition, scratches, dents etc.)

Laptop Make and Model: _____
Laptop Serial Number: _____
Employee name (please print): _____
Employee signature: _____
Date: _____

Appendix 7: Student IT Equipment Loan Assessment

ALL SAINTS SCHOOL
School Road, Lessingham, Norwich, Norfolk
NR12 0DJ
01692 582083
www.allsaintslessingham.co.uk
E-mail: office@allsaintslessingham.co.uk

Directors: Mrs J Gardiner and Mrs R Smith
Headteacher: Ms S Dangerfield

1. This agreement is between:
1) All Saints School (Lessingham) Limited ("the school")
2) [Name of parent and their address] ("the parent" and "I")
and governs the use and care of devices assigned to the parent's child (the "student"). This agreement covers the period from the date the device is issued through to the return date of the device to the school.
All issued equipment shall remain the sole property of the school and is governed by the school's policies.
1. The school is lending the student a Chromebook ("the equipment") for the purpose of attending and completing online lessons and set school
2. This agreement sets the conditions for taking an All Saints School Chromebook home.
I confirm that I have read the terms and conditions set out in the agreement and my signature at the end of this agreement confirms that I and the student will adhere to the terms of loan.

2. Damage/loss
By signing this agreement, I agree to take full responsibility for the loan equipment issued to the student and I have read or heard this agreement read aloud and understand the conditions of the agreement.
I understand that I and the student are responsible for the equipment at all times whether on the school's property or not.
If the equipment is damaged, lost or stolen, I will immediately inform Miss King (kking@allsaintslessingham.co.uk) and I acknowledge that I am responsible for the reasonable costs requested by the school to repair or replace the equipment. If the equipment is stolen, I will also immediately inform the police.

I agree to keep the equipment in good condition and to return it to the school on their demand from the school in the same condition.

I will not leave the equipment unsupervised in unsecured areas.

I will make sure my child takes the following measures to protect the device:

- Keep the device in a secure place when not in use
- Don't leave the device in a car or on show at home
- Don't eat or drink around the device
- Don't lend the device to siblings or friends
- Don't leave the equipment unsupervised in unsecured areas

3. Unacceptable use
I am aware that the school monitors the student's activity on this device.
I agree that my child will not carry out any activity that constitutes 'unacceptable use'.
This includes, but is not limited to the following:

- Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Causing intentional damage to ICT facilities or materials
- Using inappropriate or offensive language
- Searching for or viewing inappropriate material

I accept that the school will sanction the student, in line with our behaviour/discipline policy, if the student engages in any of the above **at any time.**

4. Personal use
I agree that the student will only use this device for educational purposes and not for personal use and will not loan the equipment to any other person. The equipment can only be used for the purposes of education during the hours of 9.00am-3.15pm and for completing set school work out of these hours.

5. Data protection
I agree to take the following measures to keep the data on the device protected.
- Keep the equipment password-protected – the password for the pupil logging in has been set by the school and no attempt must be made to change this. If the password has been forgotten, please contact Miss King.
- Make sure my child locks the equipment if it's left inactive for a period of time
- Do not share the equipment among family or friends

If I need help doing any of the above, I will contact Miss King on the email kking@allsaintslessingham.co.uk

6. Return date
I will return the device in its original condition to Miss King within 7 days of being requested to do so.
I will ensure the return of the equipment to the school if the student no longer attends the school.

7. Consent
[If parents are collecting the equipment]

By signing this form, I confirm that I have read and agree to the terms and conditions set out above.

STUDENT'S Full name	
PARENT'S Full name	
PARENT'S signature	

[If a signed physical copy is not able to be obtained]
By signing this form, I confirm that I have read and agree to the terms and conditions set out above.
Please sign by typing your name and your child's name.

STUDENT'S Full name	
PARENT'S full name	