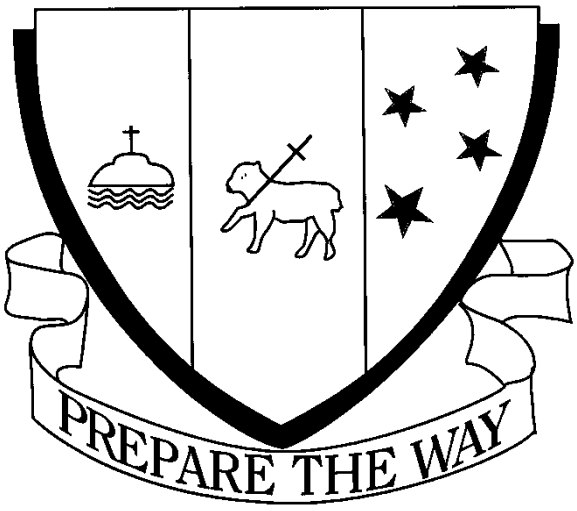
St John's School



e-Learning Procedures

Keeping Ourselves Safe Online

St John's School actively promotes good digital citizenship which includes cyber safety.

- Every child will sign a class Cybersafety Use Agreement that identifies appropriate behaviour, expectations and actions for using ICT devices. This document will also be published on the school web site and those same guidelines shall apply in this virtual space whether the student is in school or at home
- St John's School uses the Network for Learning filtration portal to block certain categories of website and filter content in the form of images and text. The Network for Learning is a government funded internet initiative.
- Students are expected to report any action, content, image or website that they find offensive, upsetting or inappropriate. They are to immediately notify the supervising adult, who will take note of the site's url and arrange for it to be blocked through the school's Computer Systems Administrator (CSA).
- Through our digital citizenship programme students at St John's will be taught the importance of managing their own digital footprint:
    - Students will be taught the importance of not sharing personal information online including the information of others
    - If individual student accounts need to be created to use a particular online service, Google Apps For Education (GAFE) for example, the school will ensure that the accounts created will not identify individual students
    - The accounts of individual students will be deleted when the student leaves the School.

Image and videos published online:

We define "online" as including but not limited to; blogs, wikis, video sharing sites, newsletters, school website, apps, social media tools such as Facebook and other third party websites.

- Images/videos that are posted online as part of a class' e-learning programme shall not identify individual children either through labelling of images or through the posting of individual images onto individual student pages.
- Where video is created in class or for school events, the individual students in the frame shall not be identified either through voice over, commentary, labelling, credits or conversation captured during the recording.
- Where practical, images of students shall be in groups greater than two.
- We have no control over images/videos of students taken by third parties including news agencies, PR companies and parents that are then posted online at promotional events or public school events such as Family Fun Night, Swimming Sports and Sports days etc

PUPIL CYBERSAFETY

Children are assisted to become safe, confident and capable e-learning users.

1. Use of the school's e-learning resources is for educational purposes only.
2. Children will be educated in Cybersafety practices, for relevant school and home e-learning use.
3. Breaches of the school Cybersafety Use Agreement will result in loss of school e-learning privileges.

Procedures

1. All children will have the signed consent of a parent/caregiver before using School e-learning equipment.

2. Year 0-2 children will have the agreement form signed by a parent or caregiver only.

3. Year 3-6 children will sign the appropriate section of the agreement form themselves.

4. Children can only go on line with permission of a supervising adult.

5. Children will be expected to use good digital citizenship practices while on line.

6. Children will have access to email via an individual account and will be given guidelines and support on the use of electronic mail.

7. In the event of a breach in the Cybersafety Use Agreement, the classroom teacher will notify the Systems Administrator immediately. The Systems Administrator will investigate the breach.

8. If, after investigation, it is determined that a breach in the Cybersafety Use Agreement has occurred, the procedures outlined in the Agreement will be implemented by the Systems Administrator.

9. Class behaviour agreements will reflect digital citizenship values explicitly in the classroom and will be displayed on class walls.

PUPIL CYBERSAFETY USE AGREEMENT

Parents/caregivers, please

- Read this document carefully (before signing) as it includes information about your responsibilities under this agreement.
- Complete and sign the page overleaf.
- Detach and return the signed Pupil Cybersafety Use Agreement page to school.
- Keep the Policy and Use Agreement documents for future reference.

Parent/Caregiver responsibilities

- I have read the Cybersafety policy and Use Agreement and understand that e-learning device use at St. John's school is for educational purposes only.

- I have gone through the Use Agreement with my child and explained its importance and that there will be consequences for breaking the Agreement.

- I will return the signed form to school so that my child can access the school's e-learning programme.

- I understand that the school has taken precautions to make Internet and email use as safe as practical, and will support the school Cybersafety policy and Use Agreement by encouraging my child to follow the Cybersafety rules.

- I understand that this agreement is binding for the time my child is enrolled at St. John's school and will retain the Use Agreement for this period.

- I understand that the class teacher will go through the Use Agreement at the commencement of each academic year before school ICT is used.

- I understand that I am welcome to contact the Systems Administrator to discuss any aspect of this Use Agreement that I might want to learn more about.

- I will become an active member of my child's class e-learning community by viewing and commenting on my child's work.

Pupil Cybersafety Use Agreement

I understand that

- St. John's school will make the Internet as safe as practical for my use.

- I can use the school network, computers and any other e-learning equipment for school work only.

- I cannot use the school e-learning equipment until my Cybersafety Use Agreement has been signed by a parent or adult who looks after me (Years 0-2) and also by myself (Years 3-6).

- I will log in to the Internet using my own username and password.

- I will log out the Internet before letting someone else use the computer.

- I will not tell my password to anyone except my parents/caregiver.
- I may use the Internet or email only under adult supervision and during class time.
- If I am not feeling safe at any time while using the computer I will turn off the screen and tell the teacher straight away. I will be shown how to minimise a window and conduct research safely and effectively according to readiness.
- The content of email will be checked by the teacher before an email is sent.
- I am not permitted to deliberately look for, copy, store or print material that is inappropriate to the Special Catholic Character and values of St. John's School. I know that if I do I will be banned from using school ICT for a period of time, and my parents will be contacted.
- I will not intentionally give anyone information about myself or others
- I will use language appropriate to the Special Character of St. John's school at all times when using school ICT.
- I understand the school can monitor my computer use, including internet and email.
- I will not download any files or programmes without the teacher's permission.
- I will have permission from home and permission from school before bringing any device (e.g flash memory, CD, iPod, camera) to school, unless it is part of my normal school equipment. I understand that the use of any devise brought from home will be at the discretion of the teacher and will be brought to school with the permission of my parents.

In addition

- I will be careful with school ICT equipment.
- If I find any faulty or broken e-learning equipment I will tell my teacher immediately.
- When communicating on line I will use good digital citizenship practices.
- If I bring a mobile phone to school it must be left at the office before school and collected after school.

St. John's School

Pupil Cybersafety Use Agreement

To be completed by a Parent/Guardian

I have read the School Cybersafety Policy and Use Agreement document carefully and am aware of the school's initiatives to maintain a Cybersafe learning environment, including the responsibilities involved. I am aware that my child will sign the student section at Year 3-6.

Name of student _____ Room _____

Name of parent/caregiver _____

Signature _____ Date _____

(Important: Parent/caregiver to complete and sign the above for ALL children, Yrs 0-6)

To be completed by the Student (Years 3-6 only)

- I have read, and / or my parents and teacher have explained, the St. John's School Cybersafety and Use Agreement.
- I agree to abide by the rules laid out in the agreement.

Student signature _____

Date _____

Name (Printed) _____

Please return to school.

Staff Technology Agreement

The welfare of staff and children is paramount when using e-learning tools.

The Internet enables staff, and children in their supervision, to gain access to information and people resources. The welfare and safety of staff is paramount when using the Internet.

Purposes

1. To provide Internet access to staff and to children in their supervision.
2. To enable staff to become safe and effective users of the Internet.
3. To integrate information from the World Wide Web and electronic mail into the school environment.
4. To facilitate inquiry based learning.
5. To provide opportunities to participate in collaborative projects.
6. To provide email for staff.
7. To encourage teachers to be active members of the school e-newspaper on our website.

Guidelines

1. Use of Internet facilities is for educational purposes, this includes personal use and use for professional development. Outside of pupil contact hours Internet facilities may be accessed for private use. Internet Access Agreement rules re. inappropriate material apply at all times. (Refer to Social Media Guidelines)
2. All staff members will abide by the terms of the Internet Content Breach Procedures.
3. Breaches of the Internet Access Agreement will be regarded as an act of serious misconduct and will be treated accordingly.
4. Access to undesirable information will be blocked by N4L and Internet access will be made as safe as practically possible.

Procedures

1. Staff will sign the Staff Computer and Internet Access Agreement before using school e-learning facilities. This document will be kept on file.
2. Using Teaching as Inquiry every teacher will be responsible for identifying and addressing areas of need in their e-learning pedagogy.
3. Teachers will use the principles of digital citizenship to enable children to become confident digital citizens in accordance with their cybersafety agreement.
4. Teachers will monitor all children's e-mail use.
5. Staff are required to abide by the Content Use Procedure. A record of all breaches will be kept by the Computer Systems Administrator (CSA) with a copy of any breach.

Computer and Internet Access Staff Agreement

I understand that:

- St. John's school will make the Internet as safe as practical for my use through a commercial filter system.
- Use of the Internet at St. John's School during pupil contact hours is strictly for educational purposes.
- Outside of contact hours Internet and email facilities may be accessed for private use.
- I am not permitted to deliberately look for, copy, store or print material that is inappropriate to the special character of St. John's school.
- I will use appropriate language at all times when using the computers and when communicating with others via Internet or email.
- The Systems Administrators have access to all communications and have the right to monitor and review all electronic content.
- No children will access the Internet or email without supervision.
- No Year 1-2 children will access the Internet or email directly.
- A breach in the agreement may result in disciplinary procedures as outlined in the Collective Employment Contract.

Staff Computer and Internet Access Agreement

Please read the statement below carefully before signing.

I have read the Staff Technology Agreement, Computer and Internet Access Staff Agreement, statement on Social Media and Internet Content Breach Agreement and agree to abide by the rules laid out in these documents.

I understand that a breach in policy and / or Internet Access Agreement rules will be regarded as an act of serious misconduct and will be treated accordingly.

Signed: _____ Date: _____

Social Media – your responsibilities

It is imperative that each staff member who uses social media understands the potential impact their actions may have on their personal and professional lives. Individual staff members need to identify where their digital boundary lies between their personal and professional lives and act accordingly. Your actions online should reflect digital citizenship best practice.

- All staff members must ensure that their actions online do not compromise the mana, integrity or reputation of St John's School

- Whilst the school understands that staff will have parents that are their friends or followers on social media sites, staff must not engage in conversations relating to school issues raised by third parties
    - Best practice in a situation where the school is being discussed online and you are privy to, is not to comment or engage with the discussions in anyway.
    - Face to face conversation is the preferred method of communication between staff and school parents. As with all school issues, concerns or enquiries team leaders and senior leadership should be notified as appropriate.

- The school understands that you have no direct control over images, videos and audio taken of you by third parties and posted to social media sites. However, the school expects that if you are in a situation where you suspect that images or videos of your actions may be posted online and may compromise the mana, integrity or reputation of St. John's School, you take reasonable precautions to ensure that they are not. Reasonable actions can include:
    - Requesting that images, video and audio are not taken of you
    - Requesting that you are not tagged in images
    - Not putting yourself in a situation where the images, videos and audio taken of you could be misinterpreted or misconstrued by others

- Please note carefully: If you bring the school into disrepute through your actions online, disciplinary action may be taken against you.

- Staff should not use their school e-mail account for any personal services on line inclusive of Facebook, Twitter and other social media sites.

Staff TELA Laptop/Tablet Agreement

In accepting the loan of a TELA laptop and tablet for the duration of my employment at St John's School, I, the undersigned agree to abide by the following conditions:

1. I understand that I have been loaned a TELA laptop and/or a tablet to be used to enhance teaching and learning opportunities for students at St John's School. I guarantee that I will exercise all due care to ensure that these devices will be kept safe and free of damage and that I am responsible at all times for ensuring they are not stolen or damaged.

2. I agree that the tablet and TELA laptop remain the property of St John's School. This equipment is only to be used by me. My children, other family members, friends and acquaintances are not permitted to use this equipment under any circumstances. Failure to comply with this clause may result in disciplinary action being taken against me.

3. I guarantee that the TELA laptop and tablet will be kept in school during the school day when the school is open, unless I am attending a conference or I am sick**.** At all other times the TELA laptop or tablet will either be securely stored at school or at my home.

4. I guarantee that if I have to leave my TELA laptop or tablet in an un-attended vehicle, the vehicle will be locked and the devices shall be out of sight in a separate, locked boot. Station wagon, hatch or van type vehicles are not secure and as such are not considered safe to leave equipment un-attended in. At all other times, when my TELA laptop or tablet are unattended I will ensure that it will be either securely locked away in my classroom or at home. Should the TELA laptop or tablet be stolen from a car that does not have a locked boot, or was not stored in one, I will be liable to pay the insurance excess of $600 on any claim.

5. I understand that while at home the TELA laptop and tablet are covered by both my home insurance and by the school's insurance. Should I not be insured at home, I understand that should the TELA laptop or tablet be stolen or damaged whilst in my care, I will have to pay the insurance excess of $600.

6. I will contact the school CSA or ICT helpdesk immediately if I have any technical problems with my TELA laptop or tablet. I will not attempt, or ask any third person who has not been authorised by the school, to make repairs or alterations to my TELA laptop or tablet. Failure to do so may result in disciplinary action being taken against you in addition to being personally liable for any repair costs.

7. Students are not permitted to use your tablet or TELA laptop in the course of the school day for teaching and learning.

8. At the conclusion of my employment, I undertake to return the computer to the school with all of the data and planning intact. I understand that the removal of personal materials at this time is my own responsibility and expense.

9. I understand that the school is not responsible for the backing up, storage or recovery of any personal files I may store on my TELA laptop or tablet, the school servers or any cloud based services the school may use. Personal files should be stored on the D drive. The loss of any personal data stored on my TELA laptop/ tablet, school servers or cloud based services used by school, that you may suffer is not the liability or responsibility of St John's School.

TELA Model: _____

TELA Serial Number_____

Tablet Model: _____

Tablet Serial Number:_____

Date:
_____

Name:
_____

Signature: _____

Internet Content Breach - Procedure

The school uses a Government approved web filtration service (Network for Learning) to ensure that only school related content is viewable in school. However, this service is not 100% accurate as new content is always being created on the web. In addition, TELA laptops and iPads move between the filtered environment of the school and the, usually, un-filtered environment of the home. Over time it is inevitable that some material that is inappropriate for school will bypass the filtration systems at school or be inadvertently accessed on TELA laptops or iPads whilst out of school. If any objectionable or offensive material is accessed on any of the Internet accessible computers the school owns, staff must do the following:

Inappropriate content breach

1. All content likely to cause offence, illegal content, non-school appropriate content discovered in but not limited to e-mails, websites, pop up pages and advertising on websites must be reported immediately to the person in charge of e-learning in the first instance and if not available the Principal.
2. You will need to state:
    a. The device the material was accessed on, including the serial number, if it is easy to access
    b. The nature of the content i.e. Gambling site, hate crime, pornographic etc
    c. The url of the site in full, don't just close the browser. If in a classroom, turn off the monitor.
    d. Where the breach occurred i.e. home, school, conference etc
    e. Who was involved
    f. What the user was doing to get to that site. I.e. "I opened an email with a link in it and it took me to the site. There was no indication in the email that this would be where I ended up."
3. All breaches are to be reported immediately if in school and within 24 hours, via e-mail to the person in charge of elearning **and** the Principal, if the event occurs off-site. Failure to report any content breach, or delay in doing so, may result in disciplinary action being taken against you.

All inappropriate content breach events will be recorded and these records will be securely stored in school for a defined period of time (7 years). These records will be kept on paper and not electronically. Each reported event will be recorded as follows:

- Date of breach
- Date breach reported
- Copy of e-mails sent, if any, attached
- Serial number of device
- Name of person reporting breach
- Name of person who accessed the content, if different from above
- Website url, copy of offending e-mail etc
- Recount of event leading to breach
- Subsequent action taken
- Signature of person reporting breach
- Signature of elearning leader or Principal
- Copy of the above given to the individual concerned for their own records

A report summary of any breaches should also be reported and minuted at the next available BoT meeting.

Class Technology Inventory St John's School

The following listed items are the e-learning tools that we have allocated to your classroom for 2015:

Device:	Model:	Serial Number:
Device:	Model:	Serial Number:
Device:	Model:	Serial Number:
Device:	Model:	Serial Number:
Device:	Model:	Serial Number:
Device:	Model:	Serial Number:
Device:	Model:	Serial Number:
Device:	Model:	Serial Number:
Device:	Model:	Serial Number:
Device:	Model:	Serial Number:
Device:	Model:	Serial Number:
Device:	Model:	Serial Number:
Device:	Model:	Serial Number:
Device:	Model:	Serial Number:
Device:	Model:	Serial Number:
Device:	Model:	Serial Number:
Device:	Model:	Serial Number:
Device:	Model:	Serial Number:
Device:	Model:	Serial Number:
Device:	Model:	Serial Number:
Device:	Model:	Serial Number:
Device:	Model:	Serial Number:

These resources are allocated to you for the duration of the year. It is your responsibility to ensure that they are returned, with all the relevant cables and chargers, as they were given to you before the end of the school year. You will be notified when in term 4 the items are to be returned.

If any item should be damaged you will need to report this immediately to Mrs Fitzgibbon our Computer Systems Administrator (CSA) so that we can get the items repaired and back to you in working order as quickly as we can.

Due to the portability and desirability of these resources there is an increased likelihood that they may be the targets of theft. It is your responsibility to ensure that when the classroom is unattended the devices are either safely locked away in a lockable cupboard or filing cabinet or attached to a locked security strap.

Please refer to the TELA agreement you signed to remind yourself of your liabilities and responsibilities with school allocated elearning resources.

Class technology resources issued by:

Name: **Signature:** **Date:**

Allocated to:

Name: **Room:** **Signature:** **Date:**

SECURITY FOR e-learning SYSTEMS ADMINISTRATION

Information and Communication Technology systems are an essential and integral part of school-wide management and pupil education at St. John's School.

- All information systems critical to the management operations of St. John's School, its hardware and software, will be as secure as possible.
- All information systems related to users will be as secure and safe as possible.

Guidelines

- The Systems Administrator and users will follow clearly defined policies and procedures.
- Information stored on the Server, placed on the Network and Laptops will be secure.
- Anti-virus software will be installed on workstations and laptops.
- N4L filtering systems will operate.
- A Systems Administrator will be responsible for I.C.T.
- A 'Support Agent' will provide further Systems administration security and troubleshooting resources, in accordance with the Service Provider's contract.
- The Network will be set up with drive mappings that will enable a range of access rights to users.
- A laptop agreement will outline procedures for Laptop use, both school and leased.
- An internet policy will outline procedures for Internet and e-mail use.
- Internet users will be protected from access to unsuitable sites.
- Only approved software will be loaded onto the system.
- The system will be backed up daily to the NAS (Network Attached Storage) Box on site. Critical data will be backed up off site and hosted by Support Agent. This is achieved by the use of Eduvault Remote Online Backup.
- A UPS (Uninterrupted Power System) is in place to manage power outages.

Procedures

- The Systems Administrator will have access rights to the server.
- The 'Support Agent' will attend St. John's school for 3 hours every week.
- The 'Support Agent' will perform routine checks as well as tasks prioritised by the Systems Administrator.

- The Support Agent will maintain a Log of work carried out on site, as guided by the Systems Administrator.
- The Server will be backed up daily.
- The Library will be backed up daily as part of the Server back up.
- Critical Data will be backed up off site and hosted by Eduvault Remote Online Backup.
- All faults will be logged to ICT Helpdesk in detail by the person finding the fault.
- The Systems Administrator will check the log daily.
- The Systems Administrator will maintain a log of work to be carried out by the Support Agent.
- Users are divided into groups.
- Group permissions will apply to each of these user groups.
- Each group of users will log on with a password.
- Teachers will have an individual log on that will remain confidential to that teacher.
- Individual passwords will remain confidential and will be changed annually.
- The Systems Administrator will maintain a confidential log of user passwords.
- The Support Agent will set up permissions for all users.
- All teachers who are allocated a Laptop will sign the Laptop Agreement (school or leased).
- All pupils and staff using the Internet will sign an Internet agreement.
- Suitable software will be installed to ensure safe online experiences for all users