## Legal and Ethical Issues related to shared information

<https://www.onslow.school.nz/application/files/2714/9626/9924/Onslow_College_Cybersafety_Use_Agreement_fromatted_June_2017.pdf>

There are laws and regulations regarding information stored on students by schools in order to ensure that -----. For example, what information are parents allowed to retrieve about their children if they call the school? What information can they retrieve on other students for that matter? Can anyone get information? What about students? Should they be able to retrieve all information on themselves? These are just some of the things that need to be considered by a school regarding their information.

### Privacy/access to information

Schools must act in loco parentis, and so they must store information about their students. This information is potentially sensitive however, so schools have guidelines and have systems in place to ensure that information is properly secured. Before we discuss how schools can safeguard their information, however, let’s first consider what information needs to be safeguarded.

Onslow College holds a whole bunch of information about the students and staff at the school which they most likely do not wish to be in the public domain. For students and staff, these include things such as family information, medical record, contact details etc. For students specifically, grades and assessments are things that they don’t want to be leaked, and for staff information such as pay rates, disputes and complaints would need to be hidden

Why would these need to be hidden? If students could freely look at other students work and grades, it could create an unhealthy environment of competition, as well as potentially raise up issues with plagiarism. If students a could view other student b’s past assessments, what’s to stop them from plagiarising their work? There’s no proof that the student b willingly helped student a with cheating, which also means that there’s no way to tell if student b did help student a.

For Teachers, looking at other’s pays could result in feelings of jealousy and inequality among other teachers, especially if only the number was able to be accessed. Even if special conditions such as training, education and experience was up in the public domain, there’s still a reasonable chance that these would be glossed over, resulting in feelings of jealousy (Papandrea, n.d.) which would then produce an unhealthy work environment.

Luckily, at Onslow College this information isn’t in the public domain. In fact, theres a whole system of permissions which dictate which pieces of information is available for teachers and students to see. At Onslow College, information is stored on PC Schools. All teachers are able to access all student’s surface information, such as their grades and/or specific pieces of medical information such as allergies. Students on the other hand, are only able to access their own grades and absences on the PC Schools web portal, and not anyone else’s. Some special individuals however, such as senior management, whanau leaders, student services and the school nurse have greater access to information about students than teachers on PC School. Generally, information is on a need to know basis. A teacher has no need to view a student’s vaccination history so they do not have access, but this information may be useful to a school nurse, so they are able to view it.

### Drives

Onslow College also has numerous shared drives, that each serve different purposes. There are 6 drives in total. The (S)tudent drive, the (H)ome drive, the Q Scanning drive, the X drive, and the N and U drives. Students are not able to see the last 2 drives as they relate to teaching materials.

The student drive is a drive that is used by all students. This drive typically contains resources relating to students, such as learning resources and/or assessment submissions. Students as a rule, except in some specific folders, can read and copy files, but are not able to write. In folders used for assessment submissions however, the opposite is true. Students are able to write files but are not able to read or even view. This is done to ensure that assessments students hand in are not seen by other students.

The home drive is a drive that is exclusive and unique to each individual student. On this drive, a student has most, if not all, of file system permissions. They can read, write, copy, view, and delete as they wish in this drive. This is because the home drive is meant for a student’s personal usage and as such they should be able to perform the operations they require in there. Students should be aware however, that other students are not access other home drives (to prevent copying) and that network managers and teachers are able to view the contents of all student home drives. Network managers, as the name implies, can check to make sure that no inappropriate content (including, but not limited to; illegal content, plagiarised material, adult content and copyrighted content). Possession of material of this nature on a school drive is a violation of the Onslow ICT Agreement and may result in the termination of their account. Teachers can also check for inappropriate content, but they can also use their view permissions to check the work of students.

The scanning drive is the drive where scanned images and files are stored. There are numerous scanners around the school that a student can use to save their physical work digitally. Everyone can view and copy, but as far as I’m aware only the scanners can write files.

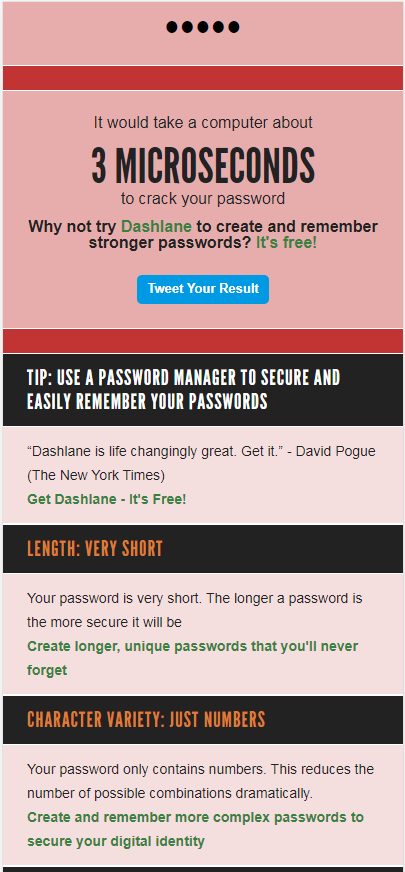
The Install drive, q, is the drive that contains the software files to be installed by ‘Zenworks’ on boot up. This file is, again, read and copy only. IT management are able to modify the files here, but otherwise there is no reason for students to use this drive.

The last 2 drives are exclusive to teachers, and students have no rights to these drives at all. This includes the ‘read’ right, which is important because these drives contain information that is in the N drive sensitive to teachers, and the U drive sensitive to all students.

N drive is the teachers common drive, similar to the students common drive. This drive contains lesson plans, faculty meeting presentations etc etc. Students are not able to access this drive, as they have no need to. Why should a student be able to view budget cuts for the language department?

The U drive is a collection of all the h drives of students. In this drive, teachers only have read access and they are unable to modify the contents of any of the student’s drives. This drive serves as a hub for teachers to navigate to a specific students drive.

### Passwords

Passwords are a method used to safeguard data to ensure that others do not get a hold of personal data. A good password is effective because it can take a long time to brute force, but when it’s weak then it becomes a vulnerability. Onslow College’s password requirements is that the chosen password has more characters than 4, with 5 being the minimum. Apart from this, there is no other special requirement such as special characters, or a variety of upper case and lower, or even numbers.

This is my current password at the time of writing this. It consists of 5 characters, all of them numbers. The password in question here is “23366”, which is an extremely insecure password. Some of the flaws, as can be seen in the attached photo, is that it contains no special characters or letters and consists of only numbers. In addition, it’s extremely short just barely making the 5 character minimum. According to How secure is my password? my current password would take 3 microseconds to brute force.

According to the cyber agreement, students are not allowed to share passwords with other students. This is done to make sure that students do not freely give each other access to their fellow peer’s drives which prevents cases of plagiarism and griefing of their materials. Teachers can change the passwords of any student, which is helpful for when a student inadvertently forgets their password and is then locked out of accessing their accounts. At Onslow College, for maximum security, students are required to log in multiple times to access different services. For example, if a student has logged into a school machine with their credentials, they are required to log in again if they wish to access PC Schools on the same machine. Even though the credentials to log into both are the same, the need to input the credentials a second time is a method of verifying that the student is the one that wishes to view their credentials, and that it’s not a random person that happened to stumble onto a student’s unlocked computer.

There are some weak points with Onslow College’s current password system however. One important security concern is that passwords at Onslow College tend to not be changed by the average student. An informal questionnaire of a 12DTM class, a class where usage of computers is heavy and they would have need to keep files on the student drive, showed that no users change their password on a regular basis. Online research shows that having periodic password resets that are mandatory in a short period of time has a detrimental effect on password security, but encouraging users to reset their password at least once in their time at Onslow College wouldn’t be a bad thing.

In addition, increasing the length of school passwords wouldn’t go amiss either. Microsoft recommends that a minimum of 8 characters for a password is a good starting point, which is already more secure than the current 5 character minimum. A extra 3 characters may not sound like much, but the increase of another character exponentially increases the amount of attempts needed to brute force a password open. Even though passwords at Onslow College aren’t stored in plaintext, these extra security measures would add another boost to Onslow College’s security.

## Backup Procedures

Backing up data is important in case of unfortunate cases when your data is threatened or lost so that you have a failsafe to work off.  Imagine certain scenarios. A student working on a assessment that accidently saves a blank document over their current one. An earthquake strikes the school and the water pipes burst, flooding the school’s server rooms. A teacher brings home their teaching laptop to mark assessments, but her cat knocks a vase over that spills water all over the laptop, short-circuiting the computer. All these scenarios would inevitable result in a loss of data, and without a backup, critical data could be lost permanently.

At Onslow College thankfully, there is a comprehensive system of backups at set intervals of time to ensure that in case any of the above disastrous scenarios occur, minimal data would be lost permanently. There are 2 main ways that Onslow College back-up data, one is on physical devices such as cassettes and on hard-drives, and the other is on the cloud using services like OneDrive which is owned and maintained by Microsoft.

But before we talk about how Onslow backups up data, let’s look at why backing up data is important for an organization such as Onslow. The student information stored on Onslow such as past assessments and grades are crucial to a student’s future. Imagine if a student’s past qualifications all completely disappeared over one night, leaving their future prospect limited! This is a bit of an extreme case, as qualifications are stored in multiple places such as NZQA, and if a disaster struck New Zealand such that all local backups are destroyed, we would have much bigger things to worry about.

The backups that are made on the cloud are done by using Microsoft’s OneDrive servers. Having a third party responsible for Onslow’s backups may sound risky but utilizing a third party in tandem with Onslow’s hard copies creates an even bigger safety net. If a calamity struck all of the Wellington region such as a earthquake for example, the cloud backups done by Microsoft would be safely stored in their Australian servers. Microsoft has more resources available meaning that they can also provide more storage. In addition, the data is then able to be accessed from anywhere in the world.

Some of the cons of this method, however, are related to the transfer of information. Since this data needs to happen over the internet, slow internet speeds could hinder the backup process, not to mention the reliance of internet connectivity. It could also potentially cost organizations heavily if their data charges get too high. If the third party that you’re utilizing to store data suddenly stops business, you may also lose all of your data. An example of this can be found in the “Mega Upload” service. A few years ago, Kim Dotcom the owner of the company got arrested which also involved the shutdown of his company. This resulted in clients having data stored on Mega Upload servers but having no way to access it.

Physical backup on the other hand, is done in a pretty continuous schedule, utilizing a series of rotations of cassette tapes in order to have the most comprehensive backups possible. For example, let’s say that Onslow College has 5 cassette tapes. On Monday, cassette tape 1 would be used to store all the data on Onslow’s servers. On Tuesday, cassette tape 2 would be used and so on and so forth. When next week comes and the next Monday comes, and there are no more available new cassette tapes, the tape with the most dated backup would then be used to back up the current data, in this case cassette tape 1. Onslow holds backups up to 2 weeks, after which the tape would be overwritten.

The tapes store around 1.5 TB of information and while this doesn’t seem enough, not everything is backed up on the cassettes. Some of the stuff that gets backed up daily includes all the changes made in a student’s s drives, but other stuff like videos on the media server or the staff drives are backed up less often meaning that less storage is necessary. In addition, data can be compressed even more, such as by utilizing the .zip file type, meaning that the 1.5 TB of storage can hold effectively 3TB of data. The tapes are stored in a different building than Onslow’s server rooms but are not taken off site.

Using cassette tapes to store Onslow’s backups has it’s pros and cons. Cassette tapes can hold a lot of data for the amount of physical space the tape takes up, which also means that it’s very portable meaning that the data can be easily taken off-site for extra security or data recovery. However, cassette tapes are slower than more modern forms of storage such as Solid-State Drives. In addition, this backup must be done manually daily meaning that there is room for human error by means of forgetting.

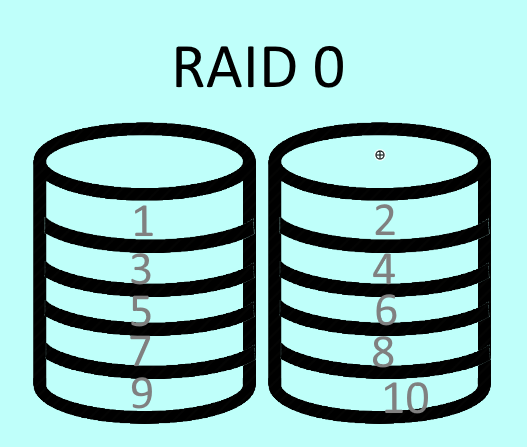
The advantages of a daily backup include protection against human error, as in our previous case of the student saving a blank over their main, and it also protects against people with more malicious intent, such as a random hacker infecting the school’s systems with ransomware. Not only can we recover the data that would have been locked away by the hacker, but we could also revert to an earlier version that wasn’t infected!

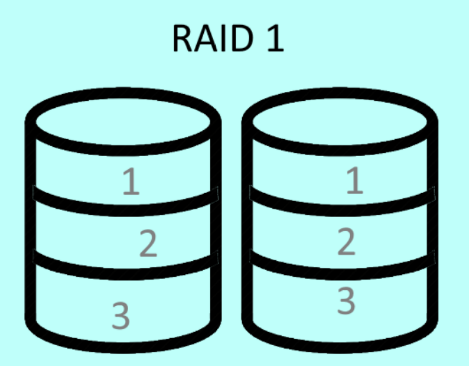
In addition to backups done on cassette tapes, there are also other storage devices that can be used such as on Onslow’s servers, external hard drives etc. Yearly backups are held on external hard drives and are located at a staff’s residence.

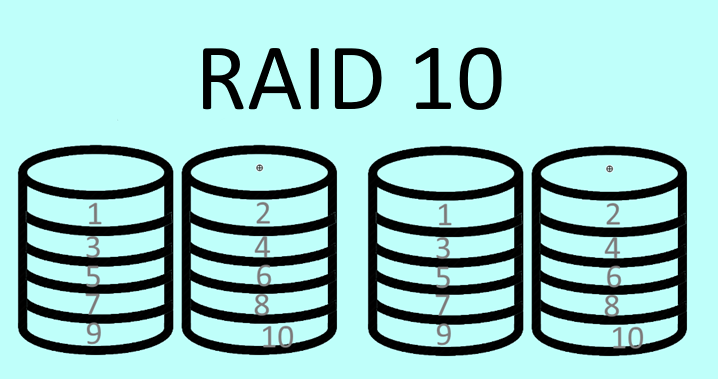
Some of the advantages of locally done backups include the cheaper costs, as organizations do not need to pay for services/internet fees. In addition, the speed would be more consistent, and data can still be access in the event of a network dropout. On the other hand, having all the backups locally reduces the amount of fail safes a company has, as if a major disaster affected the Wellington region all copies of the school’s data could be lost. In addition, locally backing up doesn’t provide the same amount of services a cloud provider could give, such as better recovery options and search.

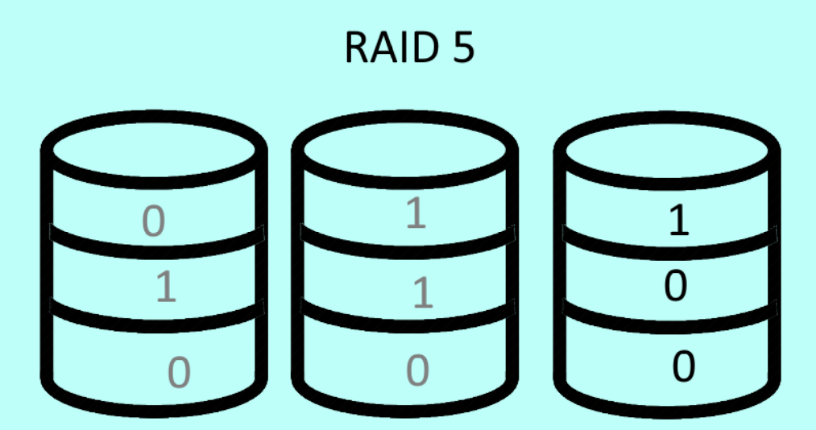
Which method of backups is more efficient, over the cloud or locally? Looking at the methods that Onslow College uses to back-up data, I think that Onslow’s current method of backing up over the cloud and locally is already an extremely robust solution. Using Microsoft’s OneDrive in tandem with a efficient system of local daily backups means that Onslow is already pretty well secured in the event of data loss.

Onslow College also uses a method of RAID array in their servers to minimize the impact of drive failure. RAID (Redundant Array of Independent/Inexpensive Disks) is a method of configuring multiple hard drives so that data is stored upon multiple disks. Onslow’s server room has a lot of hard drives in their server racks, meaning that striping data wouldn’t be hard to do. Striping data is the action of alternating data on different disks so that accessing the data will be faster due to having double the read speed.

RAID 0 as shown on the left is an example of striping data. Two disks, with an example of 10 bits evenly distributed between the disks. This is the most common RAID setup used by casual computer users, particularly in gaming as the faster read times is helpful for loading assets.

RAID 1 is like RAID 0 in that it also uses multiple disks, but instead of writing data evenly across each disk, data is written on one disk which is then mirrored by the other disk. This is called disk mirroring. While RAID 1 doesn’t reach the same speeds as RAID 0, since data is mirrored onto another disk this allows an user/organization to function normally in the event of disk failure as all traffic towards drive 1 is then directed towards drive 2. This setup is undoubtedly better for the preservation of data and is one of the more common RAID setups for organizations.

But what if we combined the speed of RAID 0 and the reliability of RAID 1? Meet RAID 10, a RAID configuration utilizing a minimum of 4 disks. As we can see in the diagram to the right, data is striped like in RAID 0 onto two different disks, and those two disks are then mirrored like in RAID 1 onto another two different disks. While this setup is undoubtedly a good combination of speed and reliability, the main issue with this setup is the cost. For every 2 drives you fill up (assuming drive 1 and drive 2 have identical storage and are being striped effectively being 1 drive) you need another 2 drives in order to mirror it.

With those costs in mind, what if we could cut down on the number of disks but still stripe and mirror data? Meet RAID 5, a compromise of RAID 10. As we can see on the diagram to the left, RAID 5 uses striping across 2 different disks to achieve the speeds of RAID 0. If you notice however, the third drive of this RAID 5 configuration seems a little different from the previous RAID 1 mirroring. That’s because RAID 5 doesn’t mirror the bits of either drives, but instead uses parity checks to check the contents of the previous two drives and then generate it’s own parity bit. How this works is that in these 3 disks, the total amount of 1s should be even. If we look at the first layer, we can see that the first two bits stored across disk 1 and 2 is a 1 and a 0 respectively. After performing a parity check, we can see that there is an odd amount of 1s, and so we generate another 1 bit in disk 3 to make the total amount even. If one of these drives were to be damaged, for example disk 1, we would be able to perform the same parity check to determine the data that was lost in disk 1. Let’s look at the second layer for example. If disk 2 has a 1 bit and disk 3 has a 0 bit, we can see that in order for disk 3 to have a 0 bit disk 1 would need to have a 1 bit to make the total amount of 1 bits equal.

One thing worth noting, is that while RAID 1 can speedily rebuild a failed drive as it’s just a simple mirror, RAID 5 does take a bit more time to rebuild as it requires parity checking to rebuild data.

Consequently, as a result of RAID 5’s lower cost but same method of striping and parity mirroring, Onslow College uses RAID 5 configuration for their servers. This has proven useful in the past as disks do fail occasionally and with this setup Onslow can rebuild the disk that has failed. In addition, this setup is faster than having individual drives which is essentially to making sure the thousand+ students at Onslow can access their drives at a reasonable speed. I think that this configuration is a great way for Onslow to minimize data loss in event of disk failure.