

Pupil Acceptable Use - Secondary

Introduction

Most of us use digital technologies daily, both within and outside school. These technologies can help your education and development by promoting creativity, curiosity, and engagement with the wider world. With an awareness of the risks involved, you should have safe access to these digital technologies and the opportunities they provide.

This Acceptable Use Agreement outlines what is expected of students when using the school's network and related technologies to maintain the safety and security of the systems and other users.

This applies to the school's computers, mobile devices such as laptops and tablets, personal devices such as mobile phones, and any activity that uses computer networks, such as the school's Wi-Fi.

Internet, apps, and email use

The school provides you with an email account and allows you to use specified apps and the Internet for educational purposes.

Whilst your school email account and devices should primarily be used for educational purposes, you may use them in a personal capacity so long as:

- It does not negatively impact the learning environment for other students and staff
- It does not damage the reputation of the school
- You understand that the school monitors your use of its network and systems, and can access your email account and Internet browsing history.

The school does not permit you to use emails, apps or the Internet in any way that could be insulting, disruptive, or offensive to someone else. Material not allowed includes, but is not limited to:

- Sexually explicit messages, images, cartoons, jokes, or movie files
- Profanity, obscenity, slander, or libel
- Ethnic, religious, political, or racial slurs

- Any content that could be seen as bullying or belittling of others based on their sex, gender, racial or ethnic origin, sexual orientation, age, disability, religious or philosophical beliefs, or political beliefs

You are also not permitted to use the Internet in a way that could affect others' usage. This means not downloading software, streaming or downloading media files such as music or films, or playing online games.

You must also be aware of copyright restrictions when using the Internet. You are not permitted to use materials in ways that would infringe intellectual property laws, including copyright. This means you should be careful when reusing online materials and content.

Security

You will take care to use accounts and systems with information security in mind. In particular, you will:

- Not click on links from untrusted or unverified sources in emails or on web pages
- Keep your passwords unique, private, and do not share them with others
- Log out when you are finished or lock your account if possible, when away from the device
- Not sign up for marketing material that could jeopardise the school's IT network
- Not send very large files without authorisation from a member of staff
- Not attempt to download any apps or software onto the school's devices or network

Monitoring

In order to support and protect students and staff, we monitor your use of the computer network, including:

- Checking and reviewing all email traffic to and from your accounts
- Monitoring your Internet and browsing activity
- Using software that blocks banned content, monitors device activity, and notifies the school of any inappropriate use or safeguarding concerns

Social media use

Using social media during school time is not permitted.

You should not use social media in a way which violates the privacy or dignity of other users, including staff, students and other members of the wider community.

Remote learning

If you are learning remotely, you may engage in more online activities than usual and be provided with accounts for more services.

All of the expectations above apply when you are accessing your school accounts from home, such as when completing home learning or in the event of remote classrooms. When learning from home, you should also:

- Not leave drinks or food near your schoolwork, computer or devices to prevent damage to work or equipment
- Only using appropriate methods to contact school staff, such as using designated school email accounts
- Remember that the school's behaviour policy and classroom expectations still apply to virtual classrooms

Safe use of online services

In addition to the safe applications the school provides for your educational use, students should take care when using online services independently. Some online services are paid for, and others are free at the point of use but are funded by advertisements. These are used at the individual's request and at the user's risk.

Online services may include:

- Apps
- Games
- Social media
- Streaming services
- Anything that offers goods and services

Students should be particularly mindful of protecting their personal information and safety when using the Internet, both within and outside school. Before using any online service, students should consider whether the service:

- Is age appropriate
- Uses child-friendly language and methods of communication
- Has high privacy settings in place by default, e.g. private rather than public profiles
- Has privacy and safety options such as blocking and reporting

- Allows you to set the user age
- Has location tracking switched off by default

These considerations help to protect and promote your safety and best interests.

Consequences of inappropriate use

Inappropriate use may result in sanctions in line with the school's behaviour policy. If you misuse the computer network and related devices, the school may:

- Remove your access to the Internet or network account
- Temporarily ban you from using school equipment
- Confiscate your personal device(s)
- Contact your parent or guardian
- Take further action, as appropriate

Pupil Acceptable Use Agreement

I have read and understand the above and agree to follow these rules when:

- I use the school systems and devices (both in and out of school).
- I use my own equipment outside of school in a way related to schoolwork, e.g. communicating with other pupils or teachers, accessing school email, website, etc.

Pupil name:

Class:

Pupil signature:

Date:

YLT Password Standards Guidance

Introduction

Passwords are used to authenticate users to access online systems and networks, and to provide the front line of defence against unauthorised access. Good password management will minimise the likelihood of user accounts being easily compromised and mitigate risks to systems that require users to log in to.

The purpose of this guidance is to set the standard for creating strong passwords. It is the user's responsibility to choose strong passwords and to keep them secure, ideally in a password manager and not within the browser's cache.

YLT Password Standards guidance is as follows:

Staff and students will have the same processes, where different rules apply, it will be stated in this guidance.

For signing into school-based networks, the following will apply:

- **Minimum length:** Students will have a minimum of 12 characters, staff will be 16 characters
- **Complexity Enabled:** Passwords to contain three of the following:
 - at least 1 Capital Letter (ABC)
 - at least 1 Lower Case Letter (abc)
 - at least 1 Number (123)
 - at least 1 Special character (!"£\$%^&*()~@.,?#':{}[]=+-)
 - Passwords cannot contain the user's name or username
- **Expiration:** Passwords are not set to expire
- **Password History:** If users are required to change their passwords, the last **10** passwords cannot be used
- **Lockout duration:** After **10** attempts of failed passwords, the user's account will lock, thus locking the user out of their network account for **15** minutes. If users require immediate access to a locked account, they need to speak to IT Support.

YLT will encourage users to use Passphrases instead of Passwords. Passphrases use multiple words that are not related to each other to form a password – for example: *Correct-Horse-Battery-Staple9*.

Passphrases are long, easy to remember and extremely difficult to decrypt.

Users that sign into online systems where YLT do not control password policies, it is recommended that users follow the above guidance.

Staff will use Multi-Factor Authentication (MFA) / 2 Factor Authentication (2FA) where possible when using online systems, if available. There is no expectation for students to use MFA (at the time of writing)

Password checking / auditing: Software tools on school networks are used to audit passwords. The software checks password requirements, breach lists or if other users in the school are using the same password. If passwords that are found to be on a breach list or not unique, the user to be notified and requested to change their password.

Associated policy or procedure: these Password Standards guidance form an appendix to the YLT Information Security Policy.