Yorkshire Learning Trust

(Legacy STAR MAT Secondary Schools)

Student Acceptable Use Policy (Secondary & 6th Form Provision)

Document History	
Created or reviewed:	Spring 2023
Reviewing officer:	The Trust Board
Review frequency:	3 Years

Approved by the Trust Board	18 July 2023
Amended to include details of AI use	17 July 2025
Review Date	July 2026

Contents

Introduction and Scope

Most of us use digital technologies every day, both within and outside school. These technologies can help your education and development by promoting creativity, curiosity, and an 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.

The **Yorkshire Learning Trust's** Acceptable Use Policy outlines what is expected of students when using the school's network and related technologies, in order to maintain the safety and security of the systems and other users.

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

Using computer accounts and the internet

The school provides you with an email account and use of the internet for educational purposes.

Personal use

Whilst your school email account 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 teaching staff,
- It does not damage the reputation of the school,
- You understand that the school has access to your email account and internet browsers, including your emails and browsing history.

Inappropriate use

The school does not permit you to send emails or use 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 or racial slurs,
- Generating and/or distributing deepfakes using Artificial Intelligence (AI),
- 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 which could affect usage for others. This means not downloading software, streaming or downloading media files such as music or films, and not using the internet for 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.

Online security

You will take care to use your accounts 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 not share these with others,
- Log out when you are finished or lock your account when away from the computer,
- Not sign up to marketing material that could jeopardise the school's IT network,
- Not send very large files without authorisation from a member of staff.
- Not install any software brought from home or downloaded from the Internet or introduce it to your own directory or anywhere else on the network without permission.

Monitoring

In order to support and protect students and staff and in line with the KCSIE's 2023 standards for filtering and monitoring, the school will monitor your use of the computer network, including:

- Checking and reviewing all email traffic that comes to and from your account,
- Monitoring your internet activity,
- Using e-monitoring software (Smoothwall) that blocks banned content, monitors internet use and can alert the school if your use looks like there is a safeguarding concern or inappropriate use.

Social media and Artificial Intelligence (AI) use

You should not use social media and Artificial Intelligence in a way which violates the privacy or dignity of other users, including staff, students and other members of the wider community. Please see the Social Media Policy.

You must not use data or information generated by electronic applications, on-line or otherwise, and claim this is your own work. This is very important regarding your work which may be assessed externally e.g. using AI to generate content for a GCSE non-examined assessment (NEA) and claiming the work is your own. Doing so is likely to mean that you would be disqualified from an external qualification (e.g. a GCSE), and possibly all qualifications from a particular examination board (e.g. AQA).

Remote learning and remote access

If the school uses remote learning, you may be engaging in more online activities than usual and provided with accounts for more services. Please see the Remote Learning Policy.

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 consider:

- Not leaving drinks or food near your school work, computer or devices – if it spills it could destroy your work or equipment,
- Only using appropriate methods to contact teachers, 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 provided by the school 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 risk of the user.

Online services may include:

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

Students are strictly prohibited from accessing gambling sites or apps during school.

When using the internet, both within and outside school, students should be particularly mindful of protecting their personal information and safety. 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.

Using age-appropriate services will help protect and promote your best interests.

Students' use of personal devices

Please see school specific mobile phone policy, which includes all types of personal devices.

Consequences of inappropriate use

Inappropriate use may result in sanctions in line with the school's Behaviour for Learning 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 parents,
- Take further action in accordance with the school's behaviour for learning policy, as appropriate.
- Recover part, or the whole cost, of damage to buildings or equipment which is the result of vandalism or negligence by a pupil or parent in line with the Charging and Remissions Policy.

By logging on and using the computers at the STAR Multi Academy Trust, you are accepting the conditions of use as laid out above and those detailed in the e-safety policy statement

Name:

Signed: Date: