Minerva
Learning Trust

# School Online Safety Policy

| | |
|---|---|
| **Date First Published** | April 2020 |
| **Version** | 2 |
| **Last Approved** | September 2021 |
| **Review Date** | September 2021 |

## Contents

# Changes to this edition

Amendment throughout from e-safety to online safety

Introduction: wider reference to the various electronic platforms

Responsibilities of the Senior Leadership Team: addition of additional AUP responsibility

Responsibilities of Technical Staff: update to include reporting incidents to Senior Leadership Team and ensuring liaison with other technical staff across the organisation

Management of Assets: amendment in relation to the requirement for IT teams to report IT disposals to the central finance team for recording on the asset register

Learning Technologies in School: updates to the use of personal email and personal equipment

# 1. Introduction

The school recognises the immense benefits that IT, the internet and a wide range of electronic communication devices and social media platforms that provide for the development of high-quality learning experiences across our school community.

We wish to actively promote engagement in the range of technologies available throughout our whole school community. With the advent of student and parental engagement through Parent Portal, a whole new level of communication and active engagement is available to us which enables us to operate within a wholly transparent and cohesive learning environment.

The school also recognises the need to balance the benefits of these technologies bring to the personal, social and health education of our students with a thorough awareness of the potential risks. It is vital that our whole school community understands and adheres to the online safety policy that ensures safe, appropriate and responsible use of such technologies and reduces the risk of exposure to adverse media and the potential impact on the mental health and wellbeing. This policy is designed to reflect our commitment to the safeguarding and wellbeing of our students.

# 2. Responsibilities of the School Community

We believe that online safety is the responsibility of the whole school community and everyone has their part to play in ensuring all members of the community are able to benefit from the opportunities that technology provides for learning and teaching. The following responsibilities demonstrate how each member of the community will contribute.

# 3. Responsibilities of the Senior Leadership Team

- Develop and promote an online safety culture within the school community.
- Ensure staff and students comply with the Acceptable Use Policy.
- Support the online safety work of the IT Support Team.
- Make appropriate resources, training and support available to members of the school community to ensure they are able to carry out their roles with regard to online safety effectively.
- Receive and regularly review online safety incident logs and be aware of the procedure to be followed should an online safety incident occur in school.
- Take ultimate responsibility for the online safety of the school community.
- Promote an awareness and commitment to online safety throughout the school.
- Implement Trust online safety policy and ensure appropriate procedures to underpin the policy are in place, monitored and embedded.
- Ensure all members of staff receive an appropriate level of training in online safety issues and their role in managing safety in the School.
- Ensure that online safety education is developed and embedded across the curriculum.
- Ensure that online safety is promoted to parents and carers.

## 4. Responsibilities of Safeguarding Manager

To play a lead role in establishing and reviewing safeguarding elements of online safety policy ensuring policy and practice reflects awareness and understanding of dangers of:

- the sharing of personal or sensitive information including sexting
- the dangers regarding access to inappropriate online contact with adults and strangers
- potential or actual incidents involving grooming of young people
- cyberbullying and the use of social media for this purpose
- online recruitment to terrorism and extremism
- Liaise with the local authority, the local safeguarding children's board and other relevant agencies as appropriate

## 5. Responsibilities of Technical Staff

- Read, understand, contribute to and help promote the school's online safety policies and guidance.
- Read, understand and adhere to the school staff Acceptable Use Policy.
- Support the school in providing a safe technical infrastructure to support learning and teaching.
- Take responsibility for the security of the school IT system including:

    - Appropriate access controls to protect personal and school sensitive data,
    - Ensure appropriate restricted network access and security
    - Restriction of administration accounts
    - Ensure appropriate detection and backup systems in place to protect essential and critical information systems to ensure recovery in event of a disaster
    - Report any online safety related issues that come to your attention to a member of the Senior Leadership Team
    - Develop and maintain an awareness of current online safety issues, legislation and guidance relevant to your work
    - Liaise with the IT central team and other technicians in relation to technical issues to ensure a swift resolution
    - Maintain a professional level of conduct in their personal use of technology at all times
    - Ensure an online safety incident log is kept up-to-date
    - Be the first point of contact in school on all online safety matters

## 6. Responsibilities of Teachers and Support Staff

- Read, understand and help promote the school's online safety policies and guidance
- Read, understand and adhere to the school staff Acceptable Use Policy
- Develop and maintain an awareness of current online safety issues and guidance
- Model safe and responsible behaviours in your own use of technology
- Embed online safety messages in learning activities where appropriate
- Supervise students carefully when engaged in learning activities involving technology
- Be aware of what to do if an online safety incident occurs
- Maintain a professional level of conduct in their personal use of technology at all times
- Computers must not be left logged on and unattended at any time

**Please note that any visitors to school who may be shadowing or supporting a department must only access the school network under supervision of a member of staff. Supply staff and volunteers who work in school regularly will receive briefing on online safety prior to being issued with logins and passwords to enable them to access the system independently.**

## 7. Responsibilities of Students

- Read, understand and adhere to the school student Acceptable Use Policy
- Agree to and sign Home School Agreement containing the onlinesafety statement
- Help and support the school in creating online safety policies and practices and adhere to any policies and practices the school creates
- Take responsibility for learning about the benefits and risks of using the Internet and other technologies in school and at home
- Take responsibility for your own and each other's safe and responsible use of technology in school and at home, including judging the risks posed by the personal technology owned and used by students outside of school
- Ensure you respect the feelings, rights, values and intellectual property of others in your use of technology in school and at home
- Understand what action you should take if you feel worried, uncomfortable, vulnerable or at risk whilst using technology in school and at home, or if you know someone who this is happening to
- Discuss online safety issues with family and friends in an open and honest way.

## 8. Responsibilities of Parents and Carers

- Help and support your school in promoting online safety
- Read, understand and promote the school student Acceptable Use Policy with your children
- Take responsibility for learning about the benefits and risks of using the Internet and other social media platforms and technologies that your children use in school and at home
- Take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies
- Discuss online safety concerns with your children, show an interest in how they are using technology, and encourage them to behave safely and responsibly when using technology and online platforms
- Model safe and responsible behaviours in your own use of technology
- Consult with the school if you have any concerns about your children's use of technology.

## 9. Responsibilities of Governing Body

- Read, understand, contribute to and help promote the school's online safety policies and guidance
- Develop an overview of the benefits and risks of the Internet and common technologies used by pupils
- Develop an overview of how the school IT infrastructure provides safe access to the Internet
- Develop an overview of how the school encourages pupils to adopt safe and responsible behaviours in their use of technology in and out of school
- Ensure appropriate funding and resources are available for the school to implement their online safety strategy.

## 10. Teaching and Learning

We believe that the key to developing safe and responsible behaviours online, not only for students but everyone within our school community, lies in effective education. We know that the Internet and other technologies are embedded in our students' lives not just in school but outside as well, and we believe we have a duty to help prepare our students to safely benefit from the opportunities the Internet brings. We will provide a series of specific online safety related lessons in every year group as part of the curriculum. We will celebrate and promote online safety through planned assemblies.

We will discuss, remind or raise relevant online safety messages with students routinely wherever suitable opportunities arise during all lessons; including the need to protect personal information, consider the consequences their actions may have on others, the need to check the accuracy and validity of information they use, and the need to respect and acknowledge ownership of digital materials.

We will ensure that all students are made aware of where to seek help or advice or make a report if they experience problems when using the internet and related technologies including social media; including how to report using CPOMS report abuse button.

We will remind students about their responsibilities through an end-user Acceptable Use Policy which every student must agree to, to allow them to use a device on first log on. The student Acceptable Use Policy will be displayed in each IT suite and displayed when students log on.

Staff will model safe and responsible behaviour in their own use of technology during lessons.

## 11. How Parents and Carers will be involved

We believe it is important to help all our parents develop sufficient knowledge, skills and understanding to be able to help keep themselves and their children safe. To achieve this, we will:

- Include useful links and advice on online safety regularly on our school website, Parent Portal and student planners
- Consult parents through parental surveys when necessary.

## 12. Managing IT Systems and Access

The school will be responsible for ensuring that access to the IT systems is as safe and secure as reasonably possible.

Servers and other key hardware or infrastructure will be located securely with only appropriate staff permitted access.

Servers, workstations and other hardware and software will be kept updated as appropriate. Virus protection is installed on all appropriate hardware, and will be kept active and up-to-date. The school will agree which users should and should not have Internet access, and the appropriate level of access and supervision they should receive.

All users will sign an end-user Acceptable Use Policy provided by the school. Users will be made aware that they must take responsibility for their use of, and behaviour whilst using the school IT systems and, that such activity will be monitored and checked.

All students will access the Internet using an individual log-on, which they will keep secure.

Whether supervised by a member of staff or working independently, students will abide by the school Acceptable Use Policy at all times.

Members of staff will access the Internet using an individual log-on, which they will keep secure. They will ensure they log-out after each session, and not allow pupils to access the Internet through their log-on. They will abide by the school Acceptable Use Policy at all times.

The school will take all reasonable precautions to ensure that users do not access inappropriate material. However, it is not possible to guarantee that access to unsuitable material will never occur.

The school will regularly audit IT use to establish if the online safety policy is adequate and that the implementation of the online safety policy is appropriate. We will regularly review our Internet access provision, and review new methods to identify, assess and minimise risks.

## 13. Filtering Internet Access

The school uses an Internet service provided by the LA. The filtering is delivered using a Smoothwall web filter device. If users discover a website with inappropriate or potentially illegal content, this should be reported to a member of staff who will inform a member of IT Support Team.

The IT Support Team will report, record and adjust filtering as required. If required, reports will be made to the Safeguarding Team and, to appropriate agencies.

The school will regularly review the filtering and other security systems to ensure they meet the needs of all users.

## 14. User Activity

The school uses software to monitor all user's activity on the school's windows workstations. The IT Support Team have access to AB Tutor to review and investigate any issues. If required reports will be made to the Safeguarding Team and to appropriate agencies.

The school will regularly review the filtering and other security systems to ensure they meet the needs of all users.

## 15. Passwords

A secure and robust username and password protocol exists for all system access. Staff and students will have a unique individually named user account and password for access to IT available within the school and via remote access.

All staff and students have a responsibility for the security of their username and password.

In line with staff and student Acceptable Use Policies users must not allow other users to access systems using their log on details and must report any suspicion or evidence of any breach of security.

## 16. Management of Assets

Details of all IT equipment, including hardware and software will be recorded in a school inventory.

All redundant IT equipment will be thoroughly checked to ensure all school related information including personal or school specific information has been thoroughly removed. All redundant IT equipment will be disposed of appropriately, including recycling with partner primaries where possible. All IT assets written off must be notified to central finance (finance@minervalearningtrust.co.uk) for noting on the asset register and reporting to Trust Board.

## 17. Learning Technologies in School

Our policy on staff and student use of a range of learning technologies is summarised in the following table. Staff and students should also refer to the Acceptable Use Policy whenever engaging with such technologies.

| | **Students** | **Staff** |
|---|---|---|
| **Student/Staff Personal mobile phones brought into school outside** | Students allowed for use outside of school site only<br>Unless school policy allows this | Staff allowed in appropriate places at appropriate times |
| **Mobile phones used in lessons** | Students not allowed unless for learning purposes | Staff allowed as part of learning activity or with permission in exceptional circumstances for private calls. |
| **Bring your own device (BYOD)** | Is permitted in line with School policy and ensuring security of the network is maintained | Is permitted in line with School policy and ensuring security of the network is maintained |
| **Taking photographs or videos on personal equipment** | Students not allowed | Staff not allowed |
| **Taking photographs or videos on school devices** | Students allowed with permission as part of a learning activity. There must be prior consent from the student under GDPR | Staff allowed as part of teaching activity. Staff Acceptable Use Policy must be followed.<br>Prior consent by the student is required under GDPR. |
| **Use of personal email addresses in school** | Students not allowed.<br>Students are provided with school email address that should be used for learning activities. | Staff allowed as long as the IT Acceptable Use Policy is followed |
| **Use of school email address for personal correspondence** | Students allowed as long as the IT Acceptable Use Policy is followed | Staff allowed as long as the IT Acceptable Use Policy is followed |
| **Use of Social Media** | Students not allowed | Staff allowed during designated breaks in appropriate places |
| **Use of Web Services** | Students allowed with permission as part of a learning activity as long as the IT Acceptable Use Policy is followed | Staff allowed as part of a school-based activity as long as the IT Acceptable Use Policy is followed |