

# 4E ONLINE SAFETY POLICY

*Reviewed: GL/SMT, Oct-Dec 2023 (Every 2 years)*

*Ratified by Trustees: December 2023*

*Next Review Date: Summer Term 2025 (as agreed by Trustees in 08/03/24 Board meeting)*

*EDI Check: SSET does not currently identify any EDI impact of this policy; should new information come to light, this will be considered at next review.*

## **1. Purpose and Scope**

This Online Safety Policy recognises the commitment of The Sheiling Ringwood (TSR) to online safety and acknowledges its integral part in the overall safeguarding policies and procedures. It shows our commitment to meeting the requirement to keep students safe when using technology.

The Online Safety Policy supports this by identifying the risks and the mitigating actions we are taking to avoid them. It shows our commitment to developing a set of safe and responsible behaviours that will enable us to reduce the risks whilst continuing to benefit from the opportunities. It ensures that all students and employees of TSR are aware that unlawful or unsafe behaviour is unacceptable and that, where necessary, disciplinary or legal action will be taken.

Online Safety is the predominant element of e-safety. E-safety is often defined as the safe and responsible use of technology. E-safety also covers the use of other means of communication using electronic media (eg. text messaging, gaming devices), interlinked areas such as data protection and the physical risks of using technology (electrocution, injury from equipment). These other elements are considered and addressed in other policies and risk assessments that support safer practices.

### **Other policies to refer to:**

- ICT Acceptable Use Policy
- Safeguarding and Child and Adult Protection Policy
- Data Protection Policy
- Code of Conduct Policy
- Visitors Policy
- Anti-bullying Policy (inclusive of cyberbullying)

As part of our commitment to online safety, we also recognise our obligation to implement a range of security measures to protect TSR network and facilities as per our Data Protection Policy.

This policy applies to the whole of TSR including the Senior Management Team (SMT), the Trustees, all staff employed directly or indirectly by TSR, volunteers, visitors and all students.

SMT and the Trustees will ensure that any relevant or new legislation that may impact upon the provision for online safety within TSR will be reflected within this policy.

SMT will ensure all members of TSR staff are aware of the contents of the online safety policy and the use of any new technology within TSR.

## **2. Who is involved in the process?**

Online safety is the responsibility of the whole of TSR 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 Principal **and DSL** has ultimate responsibility for the online safety of TSR and should:

- Identify a person (the E-Safety lead) to take day-to-day responsibility for online safety, providing them with training, monitoring and supporting them in their work.
- Receive relevant and regularly updated training in online safety to enable them to understand the risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep students safe whilst they are online.
- Ensure adequate technical support is in place to maintain a secure ICT system.
- Ensure policies and procedures are in place to ensure the integrity of TSR's information and data assets.
- Ensure online safety incidents, current issues or any trends are reported to Safeguarding Trustees.
- Ensure that all staff, students and other users agree to the ICT Acceptable Use Policy (AUP) and that new staff have online safety included as part of their induction procedures.
- Receive and regularly review online safety incident logs; ensure that the correct procedures are followed should an online safety incident occur in TSR and review incidents to see if further action is required.
- Ensure the filtering and monitoring arrangements meet DfE Filtering and monitoring standards and are reviewed for appropriateness via Senior Management Team at least annually.

### **Responsibilities of the E-Safety Lead**

- Promote an Online Safety culture throughout TSR
- Receive relevant and regularly updated training in online safety to enable them to understand the risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep students safe whilst they are online.

- Lead the Online Safety Group and maintain a running action plan on all Online Safety developments.
- Promote awareness in staff training of how to identify the types of abuse that can happen online and how technology can be used to facilitate abuse. This will include online peer on peer abuse, online bullying and sexual harassment in line with guidance from the DfE document 'KCSIE'.
- Be the first point of contact in TSR on all online safety matters.
- Take day-to-day responsibility for online safety within TSR.
- Create and maintain online safety policies and procedures.
- Develop and maintain an understanding of current online safety issues, guidance and appropriate legislation.
- Ensure that e-safety education is embedded across the curriculum, inclusive of Relationships and Sex Education (RSE).
- Ensure processes are in place to identify and manage specific risks that may be a result of a student's disability or behaviour related to ICT, inclusive of student owned personal devices
- Provide guidance and support to tailor a specific and individualised curriculum for students whom require it, these would promote resilience and reduce vulnerabilities from online safety.
- Ensure that online safety is promoted to parents and carers.
- Ensure that any person who is not a member of TSR staff, who makes use of TSR ICT equipment in any context, is made aware of the AUP.
- Liaise with the Local Authority, the Local Safeguarding Board and other relevant agencies as appropriate.
- Monitor and report on online safety issues to the Safeguarding Committee, SMT and the Safeguarding Lead, as appropriate.
- Review all internet filtering and monitoring reports for trends and concerns. Respond appropriately in terms of specific interventions and adjustments to risk assessments. Report any significant findings to Safeguarding Committee at appropriate intervals.
- Ensure that staff and students know the procedure to follow should they encounter any material or communication that makes them feel uncomfortable and how to report an online safety incident.
- Ensure online safety incidents are monitored through the Safeguarding Team.
- Promote the positive use of modern technologies and the internet.

- Ensure that TSR's Online Safety Policy and Acceptable Use Policy are reviewed at pre-arranged time intervals.

### **Responsibilities of all Staff**

- Attend Online Safety training that is mandatory for all staff (this is included within the induction programme for new staff. Update/refresher training is also mandatory, covering latest guidance within KCSiE, this policy, any related policies and any other data protection matters; a record of attendance is maintained.)
- Read, understand and help promote TSR's Policies and guidance, specifically the AUP and Data Protection Policy.
- Develop and maintain an awareness of current online safety issues, legislation and guidance relevant to their work.
- Maintain a professional level of conduct in their personal use of technology at all times.
- Ensure that all digital communication with students is on a professional level and only through TSR-based systems, never through personal accounts or by means where personal information could be compromised such as personal email addresses, phone numbers or social network accounts.
- Embed e-safety messages within learning activities where appropriate.
- Supervise students appropriately and follow guidance from documentation such as Generic Guidance when using technology or Specific Online Safety Plan for students deemed moderate to high risk as referenced in student-specific risk assessments.
- Ensure that students are given appropriate support should they encounter any material or receive a communication which makes them feel uncomfortable.
- Report all online safety incidents which occur following trained procedures and/or to their line manager in under an hour of encountering incident as per safeguarding procedures. Report any inappropriate content encountered when using the internet that may have bypassed internet filtering to the network manager in line with the process as advised in training.
- Respect intellectual property rights of others in the use of technology in TSR and at home. (Illegal copying and distribution of digital content, software, music and games)

### **Additional Responsibilities of ICT Staff**

- Support TSR in providing a safe and effective technical infrastructure to support learning and teaching.
- Report any online safety related issues to the E-Safety Lead and Designated Safeguarding Lead (DSL) or Deputies as per safeguarding procedures.

- Produce reports from internet filtering and monitoring results for the E-Safety lead to review. Track and determine source of each flagged results, highlighting areas of concern.
- Ensure that suitable access arrangements are in place for any external users of TSR's ICT equipment and these do not place the network, sensitive data or its users at significant risk.
- Ensuring the DfE Cyber security standards are met whilst providing guidance and assistance in technical procedures relating to online security and safety when arising. Review this guidance for accuracy at appropriate intervals.

### **Responsibilities of Parents and Carers**

- Help and support TSR in promoting online safety including role modelling good behaviour and practice where possible.
- Follow guidelines on the taking of video or images at TSR events.
- Be aware and vigilant of the risks of online safety.
- Know how to access online safety guidance from TSR's website to stay up-to-date with the changing risks of online safety.
- Know how to report online safety incidents externally.
- Engage and respond appropriately if a concern is raised by TSR regarding online safety and their son/daughter.
- Discuss online safety concerns with students, show an interest in how they are using technology and encourage them to behave safely and responsibly when using technology.
- Consult with the E-Safety Lead, Head of Residential Services, Head of School or College if they have any concerns about a student's use of technology.

### **Responsibilities of Trustees**

- The approval of TSR's e-safety policies and guidance as part of TSR's overarching safeguarding procedures.
- Reviewing for effectiveness of e-safety policies, this review will be informed via regular information provided to the Safeguarding Committee
- Support the work of TSR in promoting and ensuring safe use of technology in and out of TSR.
- To have an overview of how TSR's IT infrastructure provides safe access to the internet and the steps that TSR takes to protect personal and sensitive data.
- Stay up-to-date with new developments in new legislation and emerging risks from online safety.

## **Contribution of Students**

TSR acknowledges, due to the disabilities of the young people it supports, utilising the skills and knowledge of the majority students to shape curriculum and policy will be incredibly difficult to achieve. Creative mechanisms will be created for those with capabilities to contribute in a more meaningful way. This will be done in an individualised manner but may include:

- Adapted ways to canvass learner feedback and opinions regarding usage, concerns and support they feel may be needed
- Appointment of anti-bullying and online safety peer mentors
- Contribution in peer education activities such as the creation of posters and/or other content for online safety events or campaigns
- Student review and creation of individualised student acceptable use agreements

## **3. The Process**

### **Learning and Teaching**

We believe that the key to developing safe and responsible behaviours online for everyone within TSR lies in effective education. We know that the internet and other technologies are embedded in our students' lives, not just in TSR, but within the wider community. We have a duty to help prepare our students to benefit safely from the opportunities that these present and where possible build digital resilience skills.

We will deliver planned and progressive schemes of work to teach e-safety knowledge and awareness and to ensure that students have a growing understanding of how to manage the risks involved in online activity. Learning about online safety should be embedded across the waking day curriculum and also taught in specific lessons such as in ICT, PSHE and RSE.

We will discuss, remind or raise relevant online safety messages with students routinely, wherever suitable opportunities arise. This happens on a routine basis with events such as Internet Safety Day and annual online safety assemblies but, critically, in a proactive and individualised way based on student need. Assessment of each student's needs - where potential vulnerabilities are identified - directly inform a tailored learning programme. This includes the need to protect personal information and to consider the consequences their actions may have on others. Staff will model safe and responsible behaviour in their own use of technology. Students will be made aware of where to seek advice or help if they experience problems when using the internet and related technologies.

The support and learning helps prepare students to be as safe and responsible users of online technology as possible. The start and end points of their ability will differ significantly however endeavours are made for all regardless of this.

### **How parents and carers will be involved**

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

this, we will offer a range of opportunities to find out information and gain guidance. This is inclusive of any social care providers who are responsible for the care of students placed in education at the TSR.

Guidance and information can be sourced through our online safety parent / carer leaflet, meetings with TSR staff, opportunities for specific parent / carer training, TSR newsletter and our website (specifically the Online Safety page which links to a number of Online Safety organisations and has a reporting function for easy external reporting of incidents). We request that our parents support TSR in applying the Online Safety Policy.

### **Filtering Internet access**

All web traffic is monitored and web filtering ensures that all reasonable precautions are taken to prevent access to illegal content. However, it is not possible to guarantee that access to unsuitable or inappropriate material will never occur and we believe it is important to build resilience in students in monitoring their own internet activity where appropriate.

All users are informed about the action they should take if inappropriate material is accessed or discovered on a computer. However, deliberate access of inappropriate or illegal material will be treated as a serious breach of the AUP and appropriate sanctions taken.

Staff are encouraged to check out websites they wish to use prior to lessons to ascertain the suitability of content.

In the event of inappropriate content bypassing filtering systems, all staff are trained to report this to the Network Manager so filtering can continually be made more effective.

### **Using the Internet**

We provide the internet to:

- Support curriculum development in all subjects.
- Support residential students accessing internet in residential hours when using their personal devices to promote learning opportunities to practice safe use of the internet.
- Support the professional work of staff as an essential professional tool.
- Enhance TSR's management information and business administration systems.
- Enable electronic communication and the exchange of curriculum and administration data with the external agencies we work with.

Users are made aware that they must take responsibility for their use of, and their behaviour whilst using, TSR's IT systems or a Sheiling laptop or device and that such activity can be monitored and checked.

### **Dealing with Online Safety incidents**

Safeguarding incidents and abuse can take place wholly online, or technology may be used to facilitate offline abuse. Where the internet has been used to facilitate abuse or a

concern is raised involving the use of the internet that could have safety implications, this would be classified as an online safety incident.

Online safety is part of safeguarding and reporting of online safety incidents follows the same process and procedure.

All online safety incidents are recorded in the incident log which is regularly reviewed.

In situations where a member of staff is made aware of a serious online safety incident concerning students or staff, they will inform a member of the Safeguarding Team who will then respond in the most appropriate manner.

Instances of cyberbullying will be taken very seriously by TSR and dealt with using TSR's anti-bullying procedures this includes the potential for peer on peer abuse. TSR recognises that staff, as well as students, may be victims and will take appropriate action in either situation, including instigating restorative practices to support the victim. All staff are trained within induction, regular safeguarding developmental sessions, and specific updates and within the curriculum to spot concerns falling under the '4 Cs' categories – Content – Contact - Conduct – Commerce. Staff are made aware that conduct concerns may be associated or be instigated by a student at TSR.

Due to the needs and abilities of the student cohort it is unlikely that an incident would be instigated by a student and if it was the probability would be that the student would have limited capacity to understand the impact of their actions, however on any occasion a full investigation would take place via the Safeguarding team inclusive of any relevant external bodies i.e. MASH team, police, Local Authority.

TSR reserves the right to monitor equipment on their premises and to search any technology equipment, including personal equipment with permission, when a breach of this policy is suspected.

### **Dealing with a Child or Adult Protection issue arising from the use of technology:**

If an incident occurs which raises concerns about the safety of a student or the discovery of indecent images on the computer, then the procedures outlined in the Safeguarding Procedures and Guidance will be followed.

There may be occasions when the police must be contacted. Early contact will be made to establish the legal position and discuss strategies.

### **Process for monitoring the impact of the Online Safety Policy**

TSR will monitor impact of the policy and adapt where necessary using:

- Logs of incidents where identified.
- Network monitoring and filtering trends where identified.
- Surveys/questionnaires of students, staff, parents and carers

Any findings from the above will be discussed in the Online Safety group and adaptations tracked on an action plan which is reviewed by DSL team and trustee responsible for Safeguarding.