The Sheiling Ringwood

A learning and caring community where individuals are valued

4E Online Safety Policy

Policy Reviewed: GLSMT Sept-Dec 2020

Ratified by Trustees: TBC – Dec 2020

Review Date: December 2021

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 part in the overall safeguarding policies and procedures. It shows our commitment to meeting the requirement to keep students safe when using technology. We believe the entire Sheiling Ringwood community can benefit from the opportunities provided by the internet and other technologies used in everyday life.

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

As part of our commitment to online safety, we also recognise our obligation to implement a range of security measures to protect TSR's network and facilities from attack, compromise and inappropriate use and to protect TSR's data and other information assets from loss or inappropriate use.

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 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.
- 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 are reported to the Trustees.
- Develop and promote an online safety culture within TSR.
- 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.
- Make appropriate resources, training and support available to all employees of TSR to ensure they are able to carry out their roles effectively with regard to online safety.
- 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.

Responsibilities of the E-Safety Lead

- Promote an awareness and commitment to online safety throughout TSR.
- 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 an understanding of current online safety issues, guidance and appropriate legislation.
- Ensure delivery of an appropriate level of training in e-safety issues.
- Ensure that e-safety education is embedded across the curriculum.

- 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.
- Provide guidance and support to tailor a specific and individualised curriculum for students who require it in order to promote resilience and reduce vulnerabilities from online safety.
- Ensure processes and support is in place to identify and manage specific risks that may be a result of access to student-owned personal devices.
- 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 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

- Read, understand and help promote TSR's E-Safety Policies and guidance.
- Read, understand and adhere to the AUP.
- Take responsibility for ensuring the safety of sensitive data and information.
- 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 guidance and support on what to do 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.
- Ensure appropriate technical steps are in place to safeguard the security of TSR's ICT system, sensitive data and information. Review these regularly to ensure they are up-to-date.
- Ensure that provision exists for misuse detection and malicious attack.
- At the request of the SMT, conduct occasional checks on files, folders, email and other digital content to ensure that the AUP is being followed.
- Report any online safety related issues to the E-Safety Lead and Safeguarding 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 procedures are in place for new starters and leavers to be correctly added to, and removed from, all relevant electronic systems, including password management.
- 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.
- Provide guidance and assistance in technical procedures relating to online security and safety when arising. Review this guidance for accuracy at appropriate intervals.
- Ensure appropriate and regular backup procedures exist so that critical information and systems can be recovered in the event of the network or its data becoming compromised or corrupted.

Responsibilities of Parents and Carers

- Help and support TSR in promoting online safety.
- 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.
- Role model good online behaviour and practice, where possible.
- 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 or Head of School or College if they have any concerns about a student's use of technology.

Responsibilities of Trustees

- Read, understand, contribute to and help promote TSR's e-safety policies and guidance as part of TSR's overarching safeguarding procedures.
- Support the work of TSR in promoting and ensuring safe and responsible 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.

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 also when accessing in the community as well - and we believe we have a duty to help prepare our students to benefit safely from the opportunities that these present.

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

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.

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 finding 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.

Managing and safeguarding IT systems

TSR will ensure that access to its IT system is as safe and secure as is reasonably possible.

Servers and other key hardware or infrastructure are located securely with only appropriate staff permitted access. Servers, workstations and other hardware and software are kept updated, as appropriate. A firewall is maintained and virus and malware protection is installed on all appropriate hardware and is kept active and up-to-date. Staff have virus protection installed and, additionally, all laptops are encrypted against unauthorised access.

User passwords are required to be updated on a 6-monthly cycle. Passwords must be 8 or more characters in length, contain an upper case/lower case and a number. A password history of the last 4 passwords is also in force so users cannot just reuse their previous password and so are forced to change it.

All administrator or master passwords for TSR's IT systems are kept secure.

TSR's wi-fi network is protected by a secure password which prevents unauthorised access. New users wishing to connect to this wi-fi must see a member of IT Support to request authorisation in order to gain access. Residents living onsite have access to a separate and isolated wi-fi connection named 'Sheiling Residential'. This network is set up purely for internet access for residents and will not connect to the other Sheiling servers, offering total protection for TSR against malicious code or attack from potentially compromised devices not belonging to TSR.

TSR also offers guest wi-fi access in specific locations where guest access may be required; this is also an isolated link with internet access only and no other communications to the other servers.

We do not allow anyone except technical staff to download and install software onto the network.

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 in order that filtering can continually be made more effective.

Access to The Sheiling Ringwood systems

TSR decides the appropriate level of access and the level of supervision users should receive.

Restrictions to student access will only be made under careful review and due to safety or developmental reasons. Restrictions to internet access will be reviewed regularly and based on their ability to follow the Student Acceptable Usage Agreement. Restrictions to IT systems or internet access will not be used as a sanction.

There are robust systems in place for managing network accounts and passwords, including safeguarding administrator passwords. Suitable arrangements are in place for visitors to TSR who may be granted a temporary log-in.

Staff are given appropriate guidance on managing access to laptops which are used both at home and TSR and in creating secure passwords.

Access to personal, private or sensitive information and data is restricted to authorised users only, with proper procedures being followed for authorising and protecting log-in and password information. Remote access to TSR systems is covered by specific agreements and is never allowed to unauthorised third party users.

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 practise 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

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 cyber-bullying will be taken very seriously by TSR and dealt with using TSR's anti-bullying procedures. 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.

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.