

Online and E-Safety Policy

2018/19



Policy Adopted on: **09.06.2018**

Approved by: **Full Board of Trustees**

Date of Review: **08.06.2019**

Signed: _____

Contents

How to use this document

1. Creating an online safety ethos
 - 1.1. Aims and policy scope
 - 1.2. Writing and reviewing the online safety policy
 - 1.3. Key responsibilities of the community
 - 1.3.1. Key responsibilities of the management team
 - 1.3.2. Key responsibilities of the online safety/designated safeguarding lead
 - 1.3.3. Key responsibilities of staff
 - 1.3.4. Additional responsibilities of staff managing the technical environment
 - 1.3.5. Key responsibilities of children and young people
 - 1.3.6. Key responsibilities of parents/carers
2. Online communication and safer use of technology
 - 2.1. Managing the website
 - 2.2. Publishing images online
 - 2.3. Managing email
 - 2.4. Official video conferencing and webcam use
 - Users
 - Content
 - 2.5. Appropriate safe classroom use of the internet and associated devices
 - 2.6. Management of school learning platforms/portals/gateways
3. Policy decisions
 - 3.1. Recognising online risks
 - 3.2. Internet use within the community
 - 3.3. Authorising internet access
4. Engagement approaches
 - 4.1. Engagement of children and young people
 - 4.2. Engagement of children and young people who are considered to be vulnerable
 - 4.3. Engagement of staff
 - 4.4. Engagement of parents/carers
5. Responding to online incidents and concerns

June 2018

Appendix A: Procedures for responding to specific online incidents or concerns (including 'sexting', online child sexual abuse, indecent image of children, radicalisation and cyberbullying)

Appendix B: Notes on the legal framework

Appendix C: Online safety contacts and references

Appendix D: Responding to Incidents of Misuse – Flowchart

Grid for Learning.

1. Creating an Online Safety Ethos

1.1 Aims and policy scope

- Seva School believes that online safety (e-Safety) is an essential element of safeguarding children and adults in the digital world, when using technology such as computers, mobile phones or games consoles.
- Seva School identifies that the internet and information communication technologies are an important part of everyday life so children must be supported to be able to learn how to develop strategies to manage and respond to risk so they can be empowered to build resilience online.
- Seva School has a duty to provide the school community with quality Internet access to raise education standards, promote pupil achievement, support professional work of staff and enhance the school's management functions. Seva School also identifies that with this there is a clear duty to ensure that children are protected from potential harm online.
- The purpose of Seva School online safety policy is to:
 - Clearly identify the key principles expected of all members of the community with regards to the safe and responsible use technology to ensure that Seva School is a safe and secure environment.
 - Safeguard and protect all members of Seva Schools' community online.
 - Raise awareness with all members of Seva Schools' community regarding the potential risks as well as benefits of technology.
 - To enable all staff to work safely and responsibly, to role model positive behaviour online and be aware of the need to manage their own standards and practice when using technology.
 - Identify clear procedures to use when responding to online safety concerns that are known by all members of the community.
- This policy applies to all staff including the governing body, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for or provide services on behalf of the school (collectively referred to as 'staff' in this policy) as well as children and parents/carers.
- This policy applies to all access to the internet and use of information communication devices including personal devices or where children, staff or other individuals have been provided with school issued devices for use off-site, such as a work laptop or mobile phone.
- This policy must be read in conjunction with other relevant school policies including (but not limited to) safeguarding and child protection, anti-bullying, behaviour, data security, image use, Acceptable Use Policies.

1.2 Writing and reviewing the online safety policy

- Seva School online safety policy has been written by the school.
- The policy has been approved and agreed by the Leadership Team and governing body.
- The School has appointed a member of the Governing Body to take lead responsibility for online safety (e- Safety).
- The school has appointed a member of the leadership team as the online safety lead.
- The school's online safety (e–Safety) Policy and its implementation will be reviewed at least annually or sooner if required.

The School Online safety (e-Safety) Coordinator is Louisa Burnett and Antony Kay (Network Manager) The School Designated Safeguarding Lead (DSL) is Louisa Burnett

The School Online safety (e-Safety) lead for the Governing Body is Dr Amarjit Johal

Policy approved by Head of School: Date: June 2018

Policy approved by Governing Body: (Chair of Governors) Date: June 2018

The date for the next policy review is June 2019

1.3 Key responsibilities of the community

1.3.1 Key responsibilities of the school/setting management team are:

- Developing, owning and promoting the online safety vision and culture to all stakeholders in line with national and local best practice recommendations with appropriate support and consultation throughout the school community.
- Auditing and evaluating current online safety practice to identify strengths and areas for improvement.
- Supporting the online safety (e-Safety) lead in the development of an online safety culture within the setting.
- Ensuring there are appropriate and up-to-date policies and procedures regarding online safety.
- To ensure that suitable, age-appropriate and relevant filtering is in place to protect children from inappropriate content (including extremist material) to meet the needs of the school community and ensuring that the filtering and school network system is actively monitored.
- Ensuring all members of staff receive regular, up-to-date and appropriate training regarding online safety roles and responsibilities and provide guidance regarding safe appropriate communications.
- Ensuring that online safety is embedded within a progressive whole school curriculum which enables all

pupils to develop an age-appropriate understanding of online safety and the associated risks and safe behaviours.

- Making appropriate resources available to support the development of an online safety culture.
- Taking responsibility for online safety incidents and liaising with external agencies as appropriate.
- Receiving and regularly reviewing online safety incident logs and using them to inform and shape future practice.
- Ensuring there are robust reporting channels for the school/setting community to access regarding online safety concerns, including internal, local and national support.
- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology, including ensuring the safe and responsible use of devices.
- To work with and support technical staff in monitoring the safety and security of school systems and networks.
- To ensure a member of the Governing Body is identified with a lead responsibility for supporting online safety.
- To ensure that the Designated Safeguarding Lead (DSL) works in partnership with the online safety (e- Safety lead).

1.3.2 Key responsibilities of the designated safeguarding/online safety lead are:

- Acting as a named point of contact on all online safety issues and liaising with other members of staff and agencies as appropriate.
- Keeping up-to-date with current research, legislation and trends.
- Coordinating participation in local and national events to promote positive online behaviour, e.g. Safer Internet Day.
- Ensuring that online safety is promoted to parents and carers and the wider community through a variety of channels and approaches.
- Work with the school/setting lead for data protection and data security to ensure that practice is in line with legislation.
- Maintaining an online safety incident/action log to record incidents and actions taken as part of the school's safeguarding recording structures and mechanisms.
- Monitor Internet filtering reports to identify behaviour which might indicate safeguarding issues or inappropriate behaviours. Update safeguarding log or e-safety incident log as appropriate.
- Monitor the school/settings online safety incidents to identify gaps/trends and update the education response to reflect need and to report to the school management team, Governing Body and other agencies as appropriate.
- Liaising with the local authority and other local and national bodies as appropriate.
- Reviewing and updating online safety policies, Acceptable Use Policies (AUPs) and other procedures on a regular basis (at least annually) with stakeholder input.
- Ensuring that online safety is integrated with other appropriate school policies and procedures.
- Meet regularly with the governor with a lead responsibility for online safety

1.3.3 Key responsibilities of staff are:

- Contributing to the development of online safety policies.
- Reading and signing the school Acceptable Use Policies (AUPs) and adhering to them.
- Taking responsibility for the security of school/setting systems and data.
- Having an awareness of online safety issues, and how they relate to the children in their care.
- Modelling good practice in using new and emerging technologies and demonstrating an emphasis on positive learning opportunities rather than focusing on negatives.
- Embedding online safety education in curriculum delivery wherever possible.
- Identifying individuals of concern, and taking appropriate action by working with the designated safeguarding lead.
- Knowing when and how to escalate online safety issues, internally and externally.
- Being able to signpost to appropriate support available for online safety issues, internally and externally.
- Maintaining a professional level of conduct in their personal use of technology, both on and off site.
- Taking personal responsibility for professional development in this area.

1.3.4. Additional responsibilities for staff managing the technical environment are:

- Providing a safe and secure technical infrastructure which supports safe online practices while ensuring that learning opportunities are still maximised.
- Taking responsibility for the implementation of safe security of systems and data in partnership with the leadership and management team.
- To ensure that suitable access controls and encryption is implemented to protect personal and sensitive information held on school-owned devices.
- Ensuring that the school's filtering policy is applied and updated on a regular basis and that responsibility for its implementation is shared with the online safety lead and DSL.
- Ensuring that the use of Seva School network is regularly monitored in order that any deliberate or accidental misuse can be reported to the online safety lead and DSL.
- Report any breaches or concerns to the Designated Safeguarding Lead and leadership team and together ensure that they are recorded on the e Safety Incident Log, and appropriate action is taken as advised.
- Developing an understanding of the relevant legislation as it relates to the security and safety of the technical infrastructure.
- Report any breaches and liaise with Technology Team (or other local or national bodies) as appropriate on technical infrastructure issues.
- Configure internet filters to generate regular safeguarding reports, as determined by e-safety lead,

pastoral leads and DSL, and send to appropriate staff.

- Providing technical support and perspective to the online safety lead and leadership team, especially in the development and implementation of appropriate online safety policies and procedures.
- Ensuring that the school's ICT infrastructure/system is secure and not open to misuse or malicious attack.
- Ensuring that appropriate anti-virus software and system updates are installed and maintained on all setting machines and portable devices.
- Ensure that appropriately strong passwords are applied and enforced for all but the youngest users.

1.3.5 Key responsibilities of children and young people are:

- Contributing to the development of online safety policies.
- Reading the school/setting Acceptable Use Policies (AUPs) and adhering to them.
- Respecting the feelings and rights of others both on and offline.
- Seeking help from a trusted adult if things go wrong, and supporting others that may be experiencing online safety issues.

At a level that is appropriate to their individual age, ability and vulnerabilities:

- Taking responsibility for keeping themselves and others safe online.
- Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
- Assessing the personal risks of using any particular technology, and behaving safely and responsibly to limit those risks.

1.3.6. Key responsibilities of parents and carers are:

- Reading the academy's Acceptable Use Policies, encouraging their children to adhere to them, and adhering to them themselves where appropriate.
- Discussing online safety issues with their children, supporting the school in their online safety approaches, and reinforcing appropriate safe online behaviours at home.
- Role modelling safe and appropriate uses of new and emerging technology.
- Identifying changes in behaviour that could indicate that their child is at risk of harm online.
- Seeking help and support from the school, or other appropriate agencies, if they or their child encounters online problems or concerns.
- Contributing to the development of the school/setting online safety policies.
- Using school systems, such as learning platforms, and other network resources, safely and appropriately.
- Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.

2. Online Communication and Safer Use of Technology

2.1 Managing the school/setting website

- The school will ensure that information posted on the school website meets the requirements as identified by the Department for Education.
- The contact details on the website will be the school address, email and telephone number. Staff or pupils' personal information will not be published.
- The head teacher will take overall editorial responsibility for online content published by the school and will ensure that content published is accurate and appropriate.
- The school website will comply with United Learning's and the school's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.
- The school will post information about safeguarding, including online safety on the school website, or link to the resources hosted by United Learning.
- The administrator account for the school website will be safeguarded with an appropriately strong password.
- Pupils' work will only be published with their permission or that of their parents/carers.

2.2 Publishing images and videos online

- The school will ensure that all images are used in accordance with the school image use policy.
- In line with the school's image policy, written permission from parents or carers will always be obtained before images/videos of pupils are electronically published.
- Any images, videos or music posted online will comply with the intellectual property rights and copyright

2.3 Managing email

- Pupils may only use school/setting provided email accounts for educational purposes.
- All members of staff are provided with a specific school/setting email address to use for any official communication.
- The use of personal email addresses by staff for any official school/setting business is not permitted.
- The forwarding of any chain messages/emails etc. is not permitted. Spam or junk mail will be blocked and reported to the email provider.
- Any electronic communication which contains any content which could be subject to data protection legislation must only be sent using secure and encrypted methods.
- Members of the school community must immediately tell a designated member of staff if they receive offensive communication and this should be recorded in the school online safety incident log.
- Sensitive or personal information will only be shared via email in accordance with data protection legislation.
- Caution should be taken on opening emails with attachments or clicking on links within; being conscious of the risks from malware.
- Access in school to external personal email accounts may be blocked.
- Excessive social email use can interfere with learning and will be restricted.
- Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper would be.
- The school has a dedicated email for reporting wellbeing and pastoral issues. This inbox will be managed by designated and trained staff.
- School email addresses and other official contact details will not be used for setting up personal social media accounts.

2.4 Official videoconferencing and webcam use

- All videoconferencing equipment in the classroom will be switched off when not in use and where appropriate, not set to auto answer.
- The equipment will be kept securely and if necessary locked away when not in use.
- School videoconferencing equipment will not be taken off school premises without permission.
- Responsibility for the use of the videoconferencing equipment outside school time will be established with care.
- Staff will ensure that external videoconferences are suitably risk assessed and that accounts and systems used to access events are appropriately safe and secure.
- Videoconferencing is a challenging activity with a wide range of learning benefits. Preparation and evaluation are essential to the whole activity

Users

- Pupils will ask permission from a teacher before making or answering a videoconference call or message.
- Videoconferencing will be supervised appropriately for the pupils' age and ability.
- Parents and carers consent will be obtained prior to children taking part in videoconferences.
- Video conferencing will take place via official and approved communication channels following a robust risk assessment.

Content

- When recording a videoconference lesson, written permission will be given by all sites and participants. The reason for the recording must be given and the recording of videoconference should be clear to all parties at the start of the conference. Recorded material will be stored securely.
- If third party materials are to be included, the school will check that recording is acceptable to avoid infringing the third party intellectual property rights.
- The school will establish dialogue with other conference participants before taking part in a videoconference. If it is a non-school site the school will check that they are delivering material that is appropriate for the class.

2.5 Appropriate and safe classroom use of the internet and associated devices

- The school's internet access will be designed to enhance and extend education.
- Access levels to the internet will be reviewed to reflect the curriculum requirements and the age and ability of pupils.
- Pupils will use age and ability appropriate tools to search the Internet for content.
- Internet use is a key feature of educational access and all children will receive age and ability appropriate education to support and enable them to develop strategies to respond to concerns as part of an embedded whole school curriculum.
- The school will ensure that the use of Internet-derived materials by staff and pupils complies with copyright law and acknowledge the source of information.
- All members of staff are aware that they cannot rely on filtering alone to safeguard children and supervision, classroom management and education about safe and responsible use are essential.
- Supervision of pupils will be appropriate to their age and ability
 - Secondary, sixth form and college pupils will be appropriately supervised when using technology, according to their ability and understanding.
- All school owned devices will be used in accordance with the school Acceptable Use Policy and with appropriate safety and security measure in place.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- The school will use age appropriate search tools as decided by the school following an informed risk assessment to identify which tool best suits the needs of our community.

- The school will use the internet to enable pupils and staff to communicate and collaborate in a safe and secure environment.
- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school/setting requirement across the curriculum.
- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.

3. Policy Decisions

3.1. Reducing online risks

- Seva School is aware that the Internet is a constantly changing environment with new apps, tools, devices, sites and material emerging at a rapid pace.
- Emerging technologies will be examined for educational benefit and the school leadership team will ensure that appropriate risk assessments are carried out before use in school is allowed.
- The school will ensure that appropriate filtering systems are in place to prevent staff and pupils from accessing unsuitable or illegal content. Schools should include appropriate details about the systems in place.
- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer or device.
- The school will audit technology use to establish if the online safety (e–Safety) policy is adequate and that the implementation of the policy is appropriate.
- Methods to identify, assess and minimise online risks will be reviewed regularly by the school’s leadership team.
- Filtering decisions, internet access and device use by pupils and staff will be reviewed regularly by the school’s leadership team.

3.2. Internet use throughout the wider school/setting community

- The school will establish a common approach to online safety (e–Safety).
- The school will provide an Acceptable Use Policy for any guest/visitor who needs to access the school computer system or internet on site.

3.3 Authorising internet access

- The school will maintain a current record of all staff and pupils who are granted access to the school’s electronic communications.
- All staff, pupils and visitors will read and sign the School Acceptable Use Policy before using any school ICT resources.
- Parents will be informed that pupils will be provided with supervised Internet access which is appropriate to their age and ability.
- Parents will be asked to read the School Acceptable Use Policy for pupil access and discuss it with their child, where appropriate.
- When considering access for vulnerable members of the school community (such as with children with special education needs) the school will make decisions based on the specific needs and understanding of the pupil(s).

4. Engagement Approaches

4.1 Engagement and education of children and young people

- An online safety (e-Safety) curriculum will be established and embedded throughout the whole school, to raise awareness regarding the importance of safe and responsible internet use amongst pupils.
- Education about safe and responsible use will precede internet access.
- Pupils input will be sought when writing and developing school online safety policies and practices.
- Pupils will be supported in reading and understanding the school Acceptable Use Policy in a way which suits their age and ability.
- All users will be informed that network and Internet use will be monitored.
- Online safety (e-Safety) will be included in the PSHE, SRE, Citizenship and Computing programmes of study covering both safe school and home use.
- Online safety (e-Safety) education and training will be included as part of the transition programme across the Key Stages and when moving between establishments.
- The pupil Acceptable Use expectations and Posters will be posted in all rooms with Internet access.
- Safe and responsible use of the Internet and technology will be reinforced across the curriculum and within all subject areas.
- External support will be used to complement and support the school's internal online safety (e- Safety) education approaches.
- The school will reward positive use of technology by pupils.
- The school will implement peer education to develop online safety as appropriate to the needs of the pupils.

4.2 Engagement and education of children and young people who are considered to be vulnerable

- Seva School is aware that some children may be considered to be more vulnerable online due to a range of factors and will ensure that differentiated and ability appropriate online safety (e-Safety) education is given, with input from specialist staff as appropriate (e.g. SENCO).

4.3 Engagement and education of staff

- The online safety (e-Safety) policy will be formally provided to and discussed with all members of staff as part of induction and will be reinforced and highlighted as part of school safeguarding practice.
- To protect all staff and pupils, the school will implement Acceptable Use Policies which highlights appropriate online conduct and communication.
- Staff will be made aware that Internet traffic can be monitored and traced to the individual user.

Discretion and professional conduct is essential.

- Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff on a regular basis.
- Members of staff with a responsibility for managing filtering systems or monitoring ICT use will be supervised by the leadership team and will have clear procedures for reporting issues or concerns.
- The school will highlight useful online tools which staff should use with children in the classroom. These tools will vary according to the age and ability of the pupils.
- All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

4.4 Engagement and education of parents and carers

- Seva School recognise that parents/carers have an essential role to play in enabling children to become safe and responsible users of the internet and digital technology.
- Parents' attention will be drawn to the school online safety (e-Safety) policy and expectations in newsletters, letters, the school prospectus and on the school website.
- A partnership approach to online safety at home and at school with parents will be encouraged. This may include offering parent evenings with demonstrations and suggestions for safe home Internet use or highlighting online safety at other well attended events e.g. parent evenings, transition events, fetes and sports days.
- Parents will be requested to read online safety information as part of the Home School Agreement.
- Parents will be encouraged to read the school Acceptable Use Policy for pupils and discuss its implications with their children.
- Information and guidance for parents on online safety will be made available to parents in a variety of formats.
- Parents will be encouraged to role model positive behaviour for their children online.

5. Responding to Online Incidents and Concerns

- All members of the school community will be informed about the procedure for reporting online safety (e-Safety) concerns (such as breaches of filtering, cyberbullying, illegal content etc.).
- The Designated Safeguarding Lead (DSL) will be informed of any online safety (e-Safety) incidents involving child protection concerns, which will then be recorded.
- The Designated Safeguarding Lead (DSL) will ensure that online safety concerns are escalated and reported to the United Learning Designated Safeguarding Officer and relevant agencies in line with the Local Safeguarding Children Board thresholds and procedures.
- Complaints about Internet misuse will be dealt with under the School's complaints procedure.
- Complaints about online bullying will be dealt with under the School's anti-bullying policy and procedure
- Any complaint about staff misuse will be referred to the head teacher
- Any allegations against a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer).
- Pupils, parents and staff will be informed of the school's complaints procedure.
- Staff will be informed of the complaints and whistleblowing procedure.
- All members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns.
- All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community.
- The school will manage online safety (e-Safety) incidents in accordance with the school discipline/behaviour policy where appropriate.
- The school will inform parents/carers of any incidents of concern as and when required.
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes as required.
- Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact the Local Education Safeguards Team or Local Police via 999 if there is immediate danger or risk of harm.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to United Learning Technology Team and Local Police.
- If the school is unsure how to proceed with any incidents of concern, then the incident will be escalated to the United Learning Lead Safeguarding Officer or Local Education Safeguarding Team.
- If an incident of concern needs to be passed beyond the school, then the concern will be escalated to

the Local Education Safeguarding Team to communicate to other schools/settings in area.

- Parents and children will need to work in partnership with the school to resolve issues.