Shapla Primary School

Online safety Policy
October 2015

Shapla Primary School Online Safety Policy

Introduction:

It is our duty at Shapla to ensure that every child in our care is safe, and the same principles should apply to the 'virtual' or 'digital' world as would be applied to the school's physical buildings.
This Policy document is drawn up to protect all parties: the pupils, the staff and the school and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements.

Main risks for members of our school community:

- **Content**: exposure to inappropriate material (e.g. pornography and adult-rated games); lifestyle material (pro-anorexia or self-harm); hate sites (extremism)
- **Contact:** grooming (preparation for abuse); cyber-bullying; identity theft
- **Conduct**: privacy (disclosing private information); awareness of digital footprint/ tattoo; self-generated indecent images ("sexting"); health and wellbeing (excessive screen time)

Roles and Responsibilities:

Online safety Co-ordinator: Kieran Baker
Network manager: Clever ICT
Online safety Governor: Jill Hankey

The following section outlines the online safety roles and responsibilities of individuals and groups within the school.

Governors:	Governors are responsible for the approval of the Online Safety policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body / Board has taken on the role of Online safety Governor (combined role with Child Protection / Safeguarding Governor). The role of the Online safety Governor will include: • regular meetings with the Online safety Co-ordinator • regular monitoring of online safety incident logs • reporting to relevant Governors / Board / committee / meeting •
Headteacher and Senior Leaders:	• The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Online safety Co-ordinator • The Headteacher and Deputy Headteacher should be aware of the procedures to be followed in the event of a serious online

	safety allegation being made against a member of staff. • The Headteacher is responsible for ensuring that the Online safety Coordinator and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant. • The Safeguarding Officers will receive regular monitoring reports from the Online safety Co-ordinator
Online safety Coordinator	• leads the online safety committee • takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents • ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place. • provides training and advice for staff • liaises with the Local Authority / relevant body • liaises with school technical staff • receives reports of online safety incidents and creates a log of incidents to inform future online safety developments • meets regularly with Online safety Governor to discuss current issues and review incident logs • attends relevant meeting / committee of Governors / Directors • reports regularly to Senior Leadership Team
Network Manager / ICT Co-ordinator	T The Network Manager / ICT Co-ordinator are responsible for ensuring: • that the school's technical infrastructure is secure and is not open to misuse or malicious attack • that the school meets required online safety technical requirements and any Local Authority Online safety Policy / Guidance that may apply, through the LGFL filter. • that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed • the filtering policy (if it has one), is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person • that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant • that the use of the network / internet / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher / Online safety Coordinator for investigation, action and where necessary sanction • that monitoring software / systems are implemented and updated as agreed in school policies

Teaching and Support Staff	Teachers and Support Staff are responsible for ensuring that: • they have an up to date awareness of online safety matters and of the current school online safety policy and practices • they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP) • they understand the need for safeguarding all children who access materials and work online at school, linked to the Safeguarding policy • they report any suspected misuse or problem to the Headteacher / Online safety Coordinator for investigation, action and where necessary sanction • all digital communications with children, parents, carers should be on a professional level and only carried out using official school systems • online safety issues are embedded in all aspects of the curriculum and other activities • students / pupils understand and follow the online safety and acceptable use policies • they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices • in lessons where internet use is pre-planned students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
Child Protection / Safeguarding Officers	The Child Protection / Safeguarding Officer should be trained in online safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from: • sharing of personal data • access to illegal / inappropriate materials • inappropriate on-line contact with adults / strangers • potential or actual incidents of grooming • online bullying • sexual exploitation • vulnerability to radicalisation and extremism
Pupils	Pupils are responsible for • using the school digital technology systems in accordance with the Pupil Acceptable Use Policy • need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so • will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying. • should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online safety Policy covers their actions

	out of school, if related to their membership of the school
Parents / Carers	Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national / local online safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of: • digital and video images taken at school events • access to parents' sections of the website • their children's personal devices in the school (where this is allowed)
Community Users	Community Users who access school systems / website /as part of the wider school provision will be expected to sign a Community User AUA before being provided with access to school systems

.

Review: October 2016