Shevington High School

ICT Acceptable Use Policy

Pupils

DATE ADOPTED:	**October 2015**
DATE REVIEWED:	**March 2018**
COMMITTEE:	**School Effectiveness**
DATE FOR NEXT REVIEW:	**March 2019**

Shevington High School's Vision

Together we have the highest expectations for all our students, inspiring and enabling them to become amazing and successful individuals.   The Shevington Way is one of:

Shevington Standards

At Shevington High School in order to meet the school vision, Students and Adults are expected at all times to work hard to meet our *5 Shevington Standards* which we have set in order to promote respect and dignity for all*.* Our attitudes, systems and rules are drawn from and support these standards. They are:-

1. We will show respect for each other at all times

2. We will show respect for School property and another person's property at all times

3. We will show respect for ourselves and others by ensuring that our actions do not put at risk the health and safety of ourselves or others

4. We will show respect for ourselves and others by ensuring a high standard of personal appearance and organisation.

5. We will show respect for ourselves and others by supporting a positive climate for learning

Shevington High School ICT Acceptable Use Policy

The ICT Acceptable Use Policy is part of the e-safety policy. It will be reviewed at least once annually. Staff will recognise that we have moved together where individual responsibility is an essential factor in using ICT with young people and in the workplace.

The context for Acceptable Use Policies:-

In order to exploit the many educational and social benefits of new technologies, learners need opportunities to create, collaborate and explore in the digital world, using multiple devices from multiple locations. At times, they will encounter risks. It is now recognised, however, that e-safety risks are posed more by behaviours and values online than the technology itself. Our approach must therefore shift: rather than restricting access to technology, we need to empower learners and the adults who work with them to develop safe and responsible online behaviours to protect themselves whenever and wherever they go online. AUPs, when embedded within a wider framework of e-safety measures (consisting of policies, infrastructure, education and standards), can help to promote the positive behaviours needed. There is also a wider imperative for schools and other children's services to develop effective AUPs.

The Byron Review investigated the issues and opportunities for keeping children and young people safe in their use of digital technologies, and the report, Safer children in a digital world, made a series of recommendations. A subsequent action plan, published in June 2008, sets out how these recommendations will be implemented under the direction of the newly established UK Council on Child Internet Safety (UKCCIS).

One of the strategic objectives of the review is to: *Equip children to deal with exposure to harmful and inappropriate content and contact, and equip parents to help their children deal with these things and parent effectively around incidences of harmful and inappropriate conduct by their children.*

Why are AUPs important? :-

Schools are increasingly recognising the benefits of technology – and particularly Web 2.0 technologies – as an essential aspect of productive and creative social learning. However, in doing so they are finding that a blocking and banning approach which merely limits exposure to risk is no longer a sustainable approach. Children will experiment online, and while their confidence and enthusiasm for using new technologies may be high, their understanding of the opportunities and risks may be low, alongside their ability to respond to any risks they encounter. Schools now need to focus on a model of empowerment: equipping children with the skills and knowledge they need to use technology safely and responsibly, and managing the risks, wherever and whenever they go online. Effective AUPs can help to establish, and reinforce, safe and responsible online behaviours especially within the advent of virtual learning environments and networks.

Responsibilities of staff delivering the learning or care:-

Staff delivering the learning or care are essential to creating an e-safe culture, and typically have high levels of contact with the children and young people in their care and know them well. Such staff may typically be the main channel for delivering e-safety education; they may be the first point of contact should e-safety incidents occur; or may be best placed to identify changes in behaviour that may indicate that a particular individual is at risk from e-safety issues. It is essential, therefore, that they have a good awareness of the issues, and know the appropriate procedures for escalating e-safety incidents or concerns. It is also important that such staff model positive behaviours when using technologies in the learning or care environment, and adhere to staff AUPs.

Key responsibilities for teaching and support staff include:

- Contributing to the development of e-safety policies.
- Reading staff AUPs – and adhering to them.
- Taking responsibility for the security of systems and data.
- Having an awareness of e-safety issues, and how they relate to the children in their care.
- Modelling good practice in using new and emerging technologies, emphasising positive learning opportunities rather than focusing on negatives.
- Embedding e-safety education in curriculum delivery wherever possible. Identifying individuals of concern and taking appropriate action.
- Knowing when and how to escalate e-safety issues.
- Maintaining a professional level of conduct in their personal use of technology, both within and outside school.
- Taking personal responsibility for their professional development in this area

Shevington High School ICT Acceptable Use Policy (Pupils)

This agreement is designed to keep you safe whilst using the Shevington High School Networks and prevent you doing anything that could endanger others, or the software used to deliver the network.

Core AUP statements

- All users must take responsibility for their own use of new technologies, making sure that they use technology safely, responsibly and legally.
- All users must be active participants in e-safety education, taking personal responsibility for their awareness of the opportunities and risks posed by new technologies.
- No communications device, whether school provided or personally owned, may be used for the bullying or harassment of others in any form.
- No applications or services accessed by users may be used to bring the school, or its members, into disrepute.
- All users have a responsibility to report any known misuses of technology, including the unacceptable behaviours of others.
- All users agree to never use or access social network sites of staff.
- All users have a duty to respect the technical safeguards which are in place. Any attempt to breach technical safeguards, conceal network identities, or gain unauthorised access to systems and services, is unacceptable.
- All users have a duty to report failings in technical safeguards which may become apparent when using the systems and services.
- All users have a duty to protect their passwords and personal network logins, and should log off the network when leaving workstations unattended. Any attempts to access, corrupt or destroy other users' data, or compromise the privacy of others in any way, using any technology, is unacceptable.
- All users should use network resources responsibly. Wasting staff effort or networked resources, or using the resources in such a way so as to diminish the service for other n
- All users should understand that network activity and online communications are monitored, including any personal and private communications made via the school network.
- All users should be aware that in certain circumstances where unacceptable use is suspected, enhanced monitoring and procedures may come into action, including the power to check and/or confiscate personal technologies such as mobile phones.
- All users must take responsibility for reading and upholding the standards laid out in the AUP.
- All users should understand that the AUP is regularly reviewed and consistently enforced.

Specifically:-

- I will only use my own username or password to log on to the Service.
- I will keep my username and password secret.
- I will not give personal details (like my home address or mobile phone number), or the personal details of any other person, to anyone by using the network.

- I will only download, use or upload material when I have been given the owner's permission.
- I will only view, download, store, distribute or upload material that is lawful, and appropriate for other users. If I am not sure about this, or come across any potentially offensive materials, I will inform the school's ICT support team.
- I will always respect the privacy of other Users.
- I will avoid any acts of vandalism on or to the Service. This includes, but is not limited to, uploading or creating computer viruses and mischievously deleting or altering data from its place of storage.
- I will be polite and appreciate that other Users might have different views to my own. I understand that the use of strong language, swearing or aggressive behaviour is not permitted.
- I will use the discussion forums for exchanging information and constructive debate only.
- I will report any incident that breaches this Acceptable Use Policy immediately to the school's ICT support Team.
- I will only use the tools provided by the School for the purpose for which they are intended. In particular I will not use them to gain the logon details for other users or for creating defamatory material.