Online Safety Policy
Valence Primary School
January 2019

Rationale and Scope

The school believes in providing a safe and nurturing environment for pupils. This policy is intended to offer guidance and procedure for the handling and preventing of online safety related incidents as well as managing the school approach to online safety. As such, this policy is to be used in addition to other relevant policies including the Child Protection, Acceptable Use and Social Media policies.

Technology is a prevalent tool in education and can improve the quality of teaching and learning. Therefore, this policy will guide the effective use of technology in school to ensure that members of staff are confident in keeping children safe when using technology in school.

The school also strives to educate children in how to keep themselves safe and build resilience in the use of technology in all aspects of their life. The school acknowledges the duty of care for children as a global responsibility and strives to support parents in keeping children safe at home, as well as in school.

Definitions

For the purpose of this policy, technology is defined as either hardware or software, which enables pupils to communicate with others. More specifically, this policy guides the school's use of all internet based/enabled technologies, including but not limited to: iPads/mobile devices, laptops, chrome books, desktop computers, websites and online learning platforms.

While the specific intention of the policy is to inform the use of school-owned devices, guidance (including reporting procedures) may also apply to the use of personal devices where relevant; please see Acceptable Use and Data Protection policies. Pupils are not permitted to use personal devices during school hours.

Roles and Responsibilities

Online safety, as with any other form of child protection, is the responsibility of all members of staff. The Computing Coordinator, as the Designated Online Safety Lead, will work closely with the Designated Safeguarding Lead (DSL) where the roles overlap to ensure the effective adherence and updates of this policy.

The IT Team will form an additional online safety group who will monitor incidents, trends and the teaching of online safety throughout the year. This team will be responsible for evaluating online safety practice, working closely with children and parents. A group of appointed children, i.e. Digital Leaders, will also support the IT Team in the whole school approach to online safety by receiving specific training and opportunities to support their peers.

The Head teacher and governing body with liaise with the Computing Lead and the DSL to monitor online safety provision throughout the school.

While the school commits to providing young people with the knowledge and skills needed to keep themselves safe and does it's utmost to ensure that children are safeguarded in school, it is not always possible for the school to protect children who make use of the internet while at home. In this regard, the school acknowledges the role of adults with parental responsibility in monitoring children's online activity. Resources, workshops and talks are provided by the school. The school asks that responsible adults monitor and restrict children's online activity and discuss online safety regularly with them as appropriate to age. Responsible adults are asked to report all concerns related to a child's safety to the school, including online safety concerns.

The school will provide E-safety training on a regular on-going basis for all staff and those working directly with children. Further support and resources are available by contacting the Computing Lead directly.

Curriculum

Internet use is an essential element of life and children must be taught to think critically about the content they consume and create through interactions online. When utilized correctly, online technologies provide access to a wealth of information and opportunity to advance teaching and learning.

Why use the internet
- o   The internet is an essential element in education, business and social interaction and the school, therefore, has a responsibility to prepare children to make good use of technology.
- o   The school has a duty to provide children with quality internet access as a part of their learning experience as the internet is a part of the statutory curriculum.

The school will use internet-enabled technologies in a manner that:
- o   Improves access to the curriculum and engages all children.
- o   Enables teachers and children to accomplish learning outcomes, collaborate and demonstrate their learning in a variety of ways not available using 'traditional means'.

The school will ensure safe use of the internet by
- o   Filtering content and restricting access to any materials deemed inappropriate by management.
- o   Model, and ensure children adhere to responsible and respectful use of technology.
- o   Guiding the use of technology to maximize effective use for learning outcomes during lessons.
- o   Ensure communication is carried out on official school subscriptions, where it can be monitored and moderated.

Children will be taught
- o   To keep personal information safe and never give out personal details.
- o   To be wary about publishing private thoughts and/or feelings online. Children are also discouraged from sharing photos of themselves on the internet.
- o   To report and document any online activity that they are concerned about to an adult with parental responsibility, school staff or police.
- o   To behave with respect and to act in a socially responsible manner when using of technology.

Specific E-safety skills will be taught throughout the curriculum and assemblies as appropriate. These lessons will cover topics appropriate for each year group (radicalization, sexting, cyberbullying, etc.) and will vary each term to ensure a wide range of skills are covered.

Provision and Monitoring

Children at Valence are given access to a variety of internet enabled technologies. Internet traffic on school networks is filtered and monitored access to inappropriate content is restricted. All use of technology by children is monitored by the class teacher and supporting staff. SEN pupils and/or those identified as vulnerable will be additionally supervised during periods of access to the internet by a member of staff. A termly report will be produced on the school internet activity and any concerns will be reported to the governing body and Head Teacher. The Computing Lead actively participates in termly Team Around the Family meetings which acts as a Safeguarding Hub within the school.

Reporting and Guidance

Reporting concerns regarding pupils
- In the first instance, members of staff will handle any E-safety concern in line with the Behavior Policy and notify the parents/carer and Head Teacher as necessary. All incidents of online safety concerns must be recorded on CPOMS
- More serious or reoccurring concerns are to be reported and handled in line with the Child Protection Policy and may involve escalation to outside agencies if deemed necessary.
- Children can to report concerns to either a member of staff, parent or may make use of resources on the school website including the CEOP button or via the Valence worry boxes around the school.
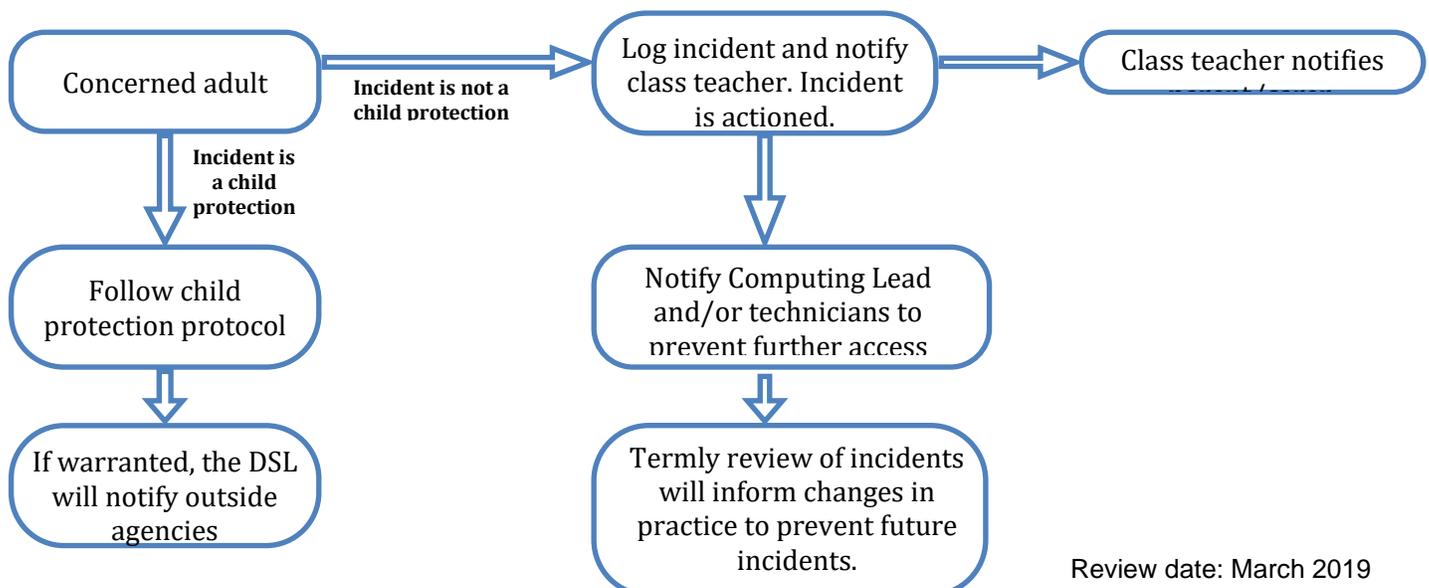
Reporting concerns regarding staff
- Concerns about the behavior or well-being of a member of staff should be reported to the Head Teacher directly and will be addressed in line with the relevant policy.

Reporting concerns from outside of the school
- Parents/carers reporting E-safety related concerns that are occurring outside of the school should report the incident to the school in the first instance.
- The school will, where possible, act to resolve the incident. If this is not possible, the incident may require referral to an outside agency (including police).

Procedure for reporting

Concerned adult

Incident is not a child protection → Log incident and notify class teacher. Incident is actioned. → Class teacher notifies parent / carer

Incident is a child protection ↓

Follow child protection protocol

↓ Notify Computing Lead and/or technicians to prevent further access

↓ If warranted, the DSL will notify outside agencies

↓ Termly review of incidents will inform changes in practice to prevent future incidents.

Review date: March 2019