COVID-19 school closure arrangements for Remote working at schools in Penk Valley Academy Trust

School Name: Penk Valley Academy Trust -all schools
Policy owner: DSL in school
Date: 2/4/2020
Date shared with staff: 3/4/2020

Context

From 20th March 2020 parents were asked to keep their children at home, wherever possible, and for schools to remain open only for those children of workers critical to the COVID-19 response - who absolutely need to attend.

Scope of the E-Safety Policy Addendum: Remote Working for Students/Pupils
This addendum applies to all members of the school community who have access to and are users of school digital technology systems out of school

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

Headteacher and Senior Leaders

- The Headteacher has a duty of care for ensuring the online safety of members of the school community

PVAT IT Team

Those with technical responsibilities 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.
- that users may only access the networks and devices through a properly enforced password protection policy
- that the use of the networks/internet/digital technologies is regularly monitored
- that monitoring software/systems are implemented and updated
- That system backups and integrity are consistent and secure

Technical – infrastructure/equipment, filtering and monitoring

The trust is responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible.

- School technical systems will be managed in ways that ensure that the school meets government guidelines
- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, routers and wireless access points must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.
- All users will be provided with a username and secure password. Users are responsible for the security of their username and password.
- Internet access is filtered and logged for all users.
- Internet filtering/monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet.
- An appropriate system is in place for users to report any actual/potential technical incident/security breach.

Teaching 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 that they have seen the staff acceptable use policy
- they report any suspected misuse or problem to the Headteacher
- all digital communications with students/pupils/parents/carers should be on a professional level and only carried out using official school systems

Pupils:

- are responsible for using the school digital technology systems in accordance with the student/pupil acceptable use agreement

- need to understand the importance of reporting abuse, misuse or problem and know how to do so
- 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 newsletters, letters, website, social media 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.
- Parents need to understand the importance of reporting abuse, misuse or problem and know how to do so.

Reporting abuse and misuse

- Any member of staff, student or parent /carer who experiences or becomes aware of online abuse, misuse or problem when using the school digital technology systems must report it immediately to the Headteacher.
- The school will make contact with each family / student at regular intervals during the closure and will ask whether there are any concerns relating to e-safety.

SAFEGUARDING INFORMATION ABOUT CALLS

- Parents need to be alerted that calls will be made- e.g.in weekly newsletter & social media. (Staff **must** get numbers from SIMS off the school system. Lists of phone numbers should not be sent out).
- If any numbers are recorded by staff to use they must be destroyed or deleted.
- Staff must use CPOMS or email the safeguarding team if there is any disclosure from a child. They should also do the same if a child is inappropriate.
- Phone numbers **must** be blocked to protect staff.
- Information on how to do this is on the hyperlink below.

https://www.wikihow.com/Hide-Your-Phone-Number-(UK)

GDPR

There are two major areas in online learning where privacy and data protection must be considered.

- **Sharing personal data via the internet**
  - Images, videos, or student submissions are all considered "personal information" under GDPR rules. It is required that any information created by students, or with them included, is anonymised, blurred out, or otherwise protected unless the parent/carer give formal permission in writing that the information can be used.
  - Children under the age of 13 must not participate in unmoderated social media activities as part of their learning.
  - If the school uses social media as part of its learning plan, the personal information of students, teachers, other staff or parents/carers should not be used or transmitted to third parties online.

- **Video conferencing and recording**
  - Just as with personal information, video imaging of minors needs permissions from parents or carers for all age groups. With learners under the age of 11, video conferencing should happen with parents / carers present.
  - As much as possible, video conferencing should be set up to eliminate backgrounds that provide information on learners' personal lives and locations. A simple white or light-coloured background is best.
  - Personal names should be avoided in any chat invites or titles. For conferences, the student and parent / carer should be informed if the conference will be recorded.
  - Health & safety must be considered if any activities involve risk (e.g. PE) if any live lessons are planned

When using any personal device (laptop, PC, tablet, phone etc) staff must ensure that files which include personal data are NOT stored on the device after use. Some online platforms and cloud storage by default download PDF files to the device on which they are being viewed. Once these are no longer required the local copy must be disposed of.