ICT and E-safety Policy

Addendum

COVID-19 school closure arrangements for ICT & E-safety

Policy addendum owner: Mark Newman Director of ICT & Data
Date: 6 April 2020 **Date shared with staff:** 14 April 2020

Context

During the current school closures due to Covid-19 there has been an unprecedented and rapid change to the expectations around ICT usage to support remote home learning.

As such this addendum covers the acceptable use of these new ways of working and will be integrated into an updated ICT & E-safety Policy in the future.

Children and online safety away from the academy/centre

Online teaching should follow the same principles as set out in the Trust's Safe Working Practice Policy which contains guidance for those working with children and young people in education settings (based on guidance from National Safer Recruitment Consortium May 2019).

The Trust will ensure any use of online learning tools and systems is in line with privacy and data protection/GDPR requirements.

Whilst staff are interacting with children away from the academy/centre online, they must continue to adhere to the Trust's Personal and Professional Conduct of Staff, Safe Working Practice Policy, ICT and E-Safety Policy and any other policies, protocols, professional standards and statutory guidance applicable to their role.

Staff should use parents' or carers' email addresses or phone numbers from the academy/centre management information system (SIMs) or academy parental engagement technologies to communicate relevant information about children, unless this poses a safeguarding risk. Use work accounts to communicate via email or online platforms, **never use personal accounts**. All remote communication with students should be done exclusively via academy/centre approved IT platforms.

In light of our change in practice due to COVID19, it may be necessary for staff to use their personal mobile phones to communicate with students, parents and carers. Where this is deemed necessary, this must be agreed by a member of the Leadership Team. Where applicable, staff should make sure any **phone calls from a personal device are made from a blocked number,** so personal contact details are not visible. Keying 141 before the phone number will block your caller ID on the call you're making.

Staff are able to access or download Trust platforms with personal devices, but must ensure that **any devices used are securely password or biometrically protected.**

If staff members are accessing families' contact details at home, ensure they comply with the Data Protection Act 2018.

Children and young people are likely to spend more time online due to social distancing. Talk to them regularly about the benefits and risks of the online world and give them space to ask questions and talk about anything that worries them.

Delivering Remote Lessons

- Remote 1:1's with students should be avoided, with students being tutored in groups wherever possible. If this is unavoidable, this must be approved by the Head of School.
- Staff and children must wear suitable clothing, as should anyone else in the household.
- Any computers used should be in appropriate areas, for example, not in bedrooms; staff need to be mindful that backgrounds do not compromise personal confidentiality or breach the guiding principles of the Trust's Safe Working Practice Policy
- The live class should be recorded so that if any issues were to arise, the video can be reviewed.
- Live classes should be kept to a reasonable length of time, or the streaming may prevent the family 'getting on' with their day.
- Language must be professional and appropriate, including any family members in the background.
- Staff should monitor any class peer to peer conversations through remote learning platforms where possible.
- Staff must only use platforms specified by senior managers and approved by our IT Director to communicate with pupils.
- Staff should record the length, time, date and attendance of any sessions held.
- Consider activities carefully when planning – online access within school has internet content filtering systems in place that are unlikely to be replicated in the home environment.
- Be careful that staff and children don't incur surprising costs, eg mobile data access charges - (video utilises significant amounts of data).

Reporting Concerns

Communicating online may allow you a view into a young person's world that you would not have seen before (and would maybe not have had the opportunity to without this crisis). This may also generate some safeguarding concerns for that young person. It is important that all staff who interact with children, including online, continue to look out for signs a child may be at risk. Any such concerns should be dealt with as per the Child Protection Policy and where appropriate referrals should still be made to children's social care and as required, the police. Any concerns must be recorded and monitored on CPOMS and a Designated Safeguarding Lead (DSL) must be informed immediately.

You will also notice if a child is not engaging in learning as required. Where this is the case, this must be reported to a member of the Leadership team so that contact can be made with the child and parent/carer, after an agreed period of time in line with your academy/centre agreed protocol, to ensure they are safe and well. Any continued concerns must be referred to the relevant organisations to ensure the safeguarding of the child.