SAFEGUARDING – GUIDANCE FOR ONLINE SAFETY AND WORKING REMOTELY

Safeguarding – guidance for online safety and working remotely

Online safety in school / the academy

It is more important than ever to provide a safe environment, including online. You must therefore take the following actions:

- continue to ensure that appropriate filters and monitoring systems (read guidance on what "appropriate" looks like) are in place to protect children when they are online on the school's / academy's IT systems or recommended resources;
- continue to follow the Trust's:
    - Policy and Procedures on Safeguarding and Child Protection
    - Acceptable Use Policy (AUP);
    - Clarification and Guidance in relation to the AUP;
    - Bring Your Own Device Policy (BYOD);
    - Staff Code of Conduct; and
    - Remote Meetings and Live Teaching Guidance
- ensure you have someone who has the technical knowledge to maintain safe IT arrangements; and
- consider what your contingency arrangements are if your IT technician becomes unavailable.

Useful websites:

The UK Council for Internet Safety https://www.gov.uk/government/organisations/uk-council-for-internet-safety provides information to help you assure that any new arrangements continue to effectively safeguard children online.

The UK Safer Internet Centre's professional online safety helpline also provides support for you with any online safety issues you may face.

Children and online safety away from school / the academy

As we envisage the provision of remote education continuing in the future, through a variety of technology solutions, particular safeguarding considerations (in addition to GDPR considerations) are required to protect you, your staff and pupils Therefore:

- ensure that in relation to any platform you have chosen, you have undertaken all necessary and relevant due diligence from a safeguarding perspective. For example; checking who can access it, what filters are in place and whether they are adequate, who has admin rights and who will be monitoring activity etc. You should also ensure that it meets GDPR requirements – *see below.*;

- only undertake 'live teaching' and / or pastoral calls in accordance with the Trust's Remote Meetings and Live Teaching Guidance;
- if you video and upload to your preferred platform, ensure you have undertaken due diligence as referred to above;
- look at the recently published guidance from the UK Safer Internet Centre on safe remote learning and from the London Grid for Learning on the use of videos as this could help in ensuring planned online lessons and/or activities are safe;
- an essential part of the online planning process should be ensuring children who are being asked to work online have very clear reporting routes in place so they can raise any concerns whilst online. As well as reporting routes back to the school / academy, you should also signpost your children to age appropriate practical support from the likes of:

  - Childline - for support
  - UK Safer Internet Centre - to report and remove harmful online content
  - CEOP - for advice on making a report about online abuse

- in terms of reporting routes back to school / the academy, it would be sensible to ensure there is a safe method for pupils to ask questions and raise concerns;
- put in place suitable risk assessments for remote learning generally, with steps in place to minimise any identified risks;
- consider what guidance you have provided to staff, pupils and parents/carers in terms of safe access to remote learning and whether any additional guidance is needed. There is DfE guidance https://www.gov.uk/government/publications/closure-of-educational-settings-information-for-parents-and-carers/closure-of-educational-settings-information-for-parents-and-carers that you can refer parents/carers to.

Protecting staff

In order to protect your staff, advise them to:

- ensure they adhere to the provisions of the Trust's Remote Meetings and Live Teaching Guidance, in particular those set out under the heading 'Teachers';
- check the content of what they are producing and/or recommending reflects the pupil cohort taking account of the needs of any vulnerable pupils (including those with SEND); and
- manage IT arrangements to ensure that they do not use their personal phones or email addresses to contact pupils / parents.

Parent/carers

You will be in regular contact with parents and carers. Such communications should be used to reinforce the importance of children being safe online. It will be especially important for parents and carers to be aware of what their children are being asked to do online, including the sites they will be asked to access

Parents and carers may choose to supplement the school / academy offer with support from online companies and in some cases individual tutors. You should emphasise the importance of securing online support from a reputable organisation/individual who can provide evidence that they are safe and can be trusted to have access to children. Support for parents and carers to keep their children safe online includes:

- Internet matters
- London Grid for Learning
- Net-aware - for support for parents and careers from the NSPCC
- Parent info
- Thinkuknow - for advice from the National Crime Agency to stay safe online
- UK Safer Internet Centre - advice for parents and carers

You should share these details with parents and carers.

Pupils with particular needs

Separate consideration should be given to pupils who may have particular needs (whether learning, emotional or otherwise) or disabilities which may make aspects of the remote learning provision particularly challenging. Together with relevant staff, consider any pupils who may have particular difficulties to consider what adjustments, strategies or support can be put in place to support them during this period, to take account of their individual circumstances.

Such arrangements must be documented on any individual pupil plans, and be monitored for effectiveness. This will help to ensure the school / academy is meeting the needs of those pupils, and mitigate against future complaints and claims for instance of a failure to make reasonable adjustments.

IT / cyber security implications

IT /cyber security implications of any online learning environment need to be thought about, with consideration given to who is able to access what. Care must be taken around permissions and extent of access granted to pupils (and staff) through the remote routes, and content should be suitable for the age of the pupils accessing it.

These considerations should be documented and kept with any other school / academy risk assessments. The strategies and measures taken in relation to these risks should also be documented and monitored.

GDPR

Right now, in the midst of Covid-19, GDPR may not feature strongly (or at all) on schools' lists of considerations. But there are 2 big reasons why it should:

- protecting personal data remains a statutory obligation under GDPR, regardless of whether it is being processed onsite or offsite. (Remember, under GDPR, you have a statutory obligation to take appropriate technical and organisational measures to protect personal data); and
- new data security risks are likely to emerge as attackers exploit the Covid-19 crisis to launch new phishing attacks and identify vulnerabilities in your security measures.

Actions/measures to be taken/checked:

- ensure any use of online learning tools and systems is in line with privacy and data protection/GDPR requirements – if in doubt, check with the PDET Central Team;
- remind staff that they must not use their own personal devices for work (this includes accessing emails from their own personal smartphone, or working from a home PC, or personal laptop) without specific permission - *see the Trust's Bring Your Own Device Policy (BYOD)* for more information as to the conditions for the granting of any permission. Under no circumstances should individual pupil data be stored on any personal device. Every teacher should be using their school / academy device;
- remind all staff of their obligation to protect personal data when working away from the building;
- remind all staff that data breaches can cause real and significant harm to individuals and result in enforcement action (including substantial fines), adverse publicity and unwanted scrutiny. Any data breaches must immediately be reported to the DPO in the usual way – dpo.pdet@peterborough-diocese.org.uk. If you are unsure whether there is potentially a breach – contact the PDET Central Team;
- remind staff that they must check that any device that is used, is protected with end point security such as up to date Antivirus, malware and Personal Firewalls etc.
- all staff to re-read the Staff Code of Conduct, AUP, Clarification and Guidance in relation to the AUP and the Remote Meetings and Live Teaching Guidance;
- staff to watch the PDET webinar on GDPR if they have not already done so, or need to refresh their knowledge;
- remind staff that any device that is used to store or process personal data must be encrypted with a password (noting that not all passwords double up as encryption);
- remind staff that they must protect personal data from being accessed or seen by others including friends, family and the public and must not share passwords or access credentials;
- remind staff that they must lock their screen when stepping away from the device. They must also log off at the end of working and ensure that personal data is locked away; and
- alert staff to be vigilant against emerging new risks such as phishing attacks.

Staff meetings/CPD etc. held/delivered virtually

For those schools / academies that have Microsoft Teams, we would recommend using this for such meetings. For those of you who do not have Teams, we would suggest using Zoom, provided you follow the rules set out below:

- **Use the latest version of Zoom** – currently – January 2020.
- **Set up a meeting ID** – do not use your personal ID (PMI) to host. Instead, use a randomly generated meeting ID. (*To do this, click on 'Schedule' and make sure 'use personal ID' is not selected*). Also ensure a password is required to enter the meeting. *Make sure that the password is only shared to access the meeting privately i.e. via email*.
- **Lock the meeting** – if it is a staff meeting, once the meeting has started and all participants joined, lock the meeting. This means that nobody else can join the meeting even if they have the meeting ID. *This can be found in meeting settings.*
- **Monitor participants** – Zoom allows for a participant's video and audio to be turned off by tapping on either option in the participant menu.
- **Use the waiting room** – this means participants have to wait in a virtual waiting room before joining the meeting. A personalised message can be added to this area, perhaps setting ground rules. It also allows the person in charge of the meeting to check who is in the waiting room before allowing them into the meeting.
- **No personal information is to be mentioned**.
- **The meeting will not be recorded unless it is a training session and then provided all attendees are in agreement** – by default, this option is disabled.
- **Ensure everybody understands that the meeting and its link must not be published on Social media**.