Peterborough Diocese Education Trust

ACHIEVING MORE TOGETHER

REMOTE EDUCATION: ONLINE SAFETY

(Safeguarding and GDPR considerations)

Guidance for schools / academies

Updated January 2021

Remote Education: Online Safety

(Safeguarding and GDPR considerations)

Guidance for schools / academies

Online safety

It is more important than ever with the move to remote education 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, platforms 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

  you should also be aware of the provisions of the Trust's Remote Education: Guidelines for Parents / Carers and Pupils;

- 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 continue with the provision of remote education, through a variety of technology solutions, particular safeguarding considerations (in addition to GDPR considerations) are required to protect you, your staff and pupils.

General recommendations:

- put in place suitable risk assessments for remote education from a technical, curriculum, data protection and safeguarding point of view, with steps in place to minimise any identified risks;
- ensure that any devices that children are given to use at home are suitably set up and equipped with appropriate filtering and monitoring software;
- if devices have been donated or repurposed, ensure that they have been completely wiped and are clear of any old files, apps and data before giving to children;
- 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 GDPR section below*;
- platforms should be set up securely by you to prevent unauthorised access;
- train staff prior to any new platforms being used with children so they have knowledge of the key functions as well as behaviour expectations;
- only undertake 'live' teaching and / or pastoral calls in accordance with the conditions set out below;
- look at the 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;
- consider what guidance you have provided to staff, pupils and parents/carers in terms of safe access to remote education 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.

What is expected in relation to 'live' teaching and remote meetings, including pastoral calls undertaken by school / academy staff:

It is expected that when conducting 'live' teaching, support staff will be responsible for the technical aspects enabling the teacher to teach.

- Parents / carers will have already seen the Trust's Remote Education: Guidelines for Parents / Carers and Pupils, which sets out expectations both for parents / carers and pupils.
- Teachers will only use platforms and communication channels approved by the Trust to deliver remote education.
- Teachers will 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);
- Teachers will ensure that only pupils who have received parental / carer approval participate in live sessions.
- Teachers will ensure that they show pupils how to access live sessions and that they understand the protocol and expectations when participating in live sessions.
- Live sessions must only take place during core school / academy hours.
- Teachers must provide details of when 'live' lessons will take place and when they will end on the school's / academy's platform so that parents / carers are aware.
- Teachers should give at least 24 hours' notice of any planned pastoral calls prior to the 'live' session.
- Teachers will only proceed with a 'live' lesson if there is a minimum of 3 pupils present (including those pupils on-site).
- Teachers will ensure that, when making pastoral calls, there is a minimum of 2 school staff members present and that the child's parent / carer is together with the child throughout the duration of the call.
- Teachers will only use online platforms such as Zoom, Microsoft Teams or Google Classroom set up with their school / academy provided email address.
- Teachers will **contact parents and pupils through school / academy email only**.
- Teachers will obtain the Headteacher's consent for any pastoral call.
- Before hosting live sessions on Zoom, Microsoft Teams or Google Classroom, teachers must have accessed the school's / academy's CPD and have familiarised themselves with all the tools available for them to use in order to enhance the security and privacy of their session.
- Teachers will keep a record of the live sessions (date, time, length, topics).
- Teachers will keep a register of those children who have accessed 'live' lessons on the agreed school / academy format.
- Teachers will ensure pupils abide by the school's / academy's *Internet Acceptable Usage Policy* and Behaviour Policy at all times.
- Teachers will conduct sessions in a professional manner and in accordance with the Trust's Staff Code of Conduct, including being suitably attired during live sessions and ensuring they are broadcast from an appropriate location.

- If conducting sessions from home, teachers will ensure family members, and anyone else who is not a member of staff, are out of the room during live sessions.
- Where possible, cameras should be used against a neutral background, with the light source directed towards the instructor's face and no personal items should be in sight.
- At the end of a session the teacher will advise **all pupils to leave the session** and when all pupils have left, the teacher can then end the session.
- Teachers will ensure any personal data used or captured when delivering remote learning is processed and stored in accordance with data protection requirements and any suspected data breaches are reported to the DPO (and the Headteacher).
- Teachers will ensure that, where they are directing children to content from another provider, they quality assure the content and provider beforehand to check that it is safe, suitable and appropriate.
- All staff will manage IT arrangements to ensure that they do not use their personal phones or email addresses to contact pupils / parents.

- **When using Zoom**, teachers will ensure / undertake the following:

    - **Use the latest version of Zoom** – they will ensure they are using the latest updated version of Zoom.
    - **Set up a meeting ID** – they will not use their personal ID (PMI) to host. Instead, they will use a randomly generated meeting ID. (*To do this, click on 'Schedule' and make sure 'use personal ID' is not selected*). Also they will 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*.
    - **Mute attendees on joining** – camera and microphone.
    - **Lock the meeting** – once the meeting has started and all participants joined, the meeting will be locked. This means that nobody else can join the meeting even if they have the meeting ID. *This can be found in meeting settings.*
    - **Consider disabling private chat / content** - Zoom offers the ability for participants to chat / message each other privately. Consider disabling this option in meeting settings. The ability for participants to share content in meeting settings can also be disabled.
    - **Restrict Screen sharing** so that participants can't take control and share content with the rest of the group.
    - **Monitor participants** – Zoom allows for a participant's video and audio to be turned off by tapping on either option in the participant menu. Teachers will

ensure they know how to remove unwanted or disruptive participants as well (*found in the participants' menu*) should they need to.

- **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**.
- **Everybody understands that the meeting and its link must not be published on Social media**.

- **When using Microsoft Teams**, teachers will ensure / undertake the following:

  - **Double check that any other tabs open** in the browser would be appropriate for a child to see, if the screen is being shared;
  - **Consider disabling chat** for pupils;
  - **Make use of the 'meeting lobby'** meaning pupils need to be admitted to the session;
  - **Ensure pupils join as 'attendees'** so their functionality is controlled;
  - **Switch off the setting** of 'Anonymous users can join a meeting' (pupils will need to be signed into Teams to access);
  - **Remove a pupil's ability** to schedule meetings, create live events, and participate in private calls within the settings;

- **When using Google Classroom,** teachers will ensure / undertake the following:

  - **Familiarise themselves with the security controls** such as muting or removing participants;
  - **Schedule meetings in Google calendar** so only those on the calendar invite can join and pupils cannot re-join once the final attendee has left;
  - **Double check that any other tabs open in the browser** would be appropriate for a child to see, if the screen is being shared;
  - **Consider disabling Google Chat** for pupils.

Parents/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 is especially important for parents and carers to be informed of what their children are being asked to do online, including which websites and apps they are being asked to use as well as which member(s) of staff their child will be contacted by or will interact with.

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.

Third party providers

The following third parties providing tutoring, interventions and / or coaching are part of the NTP and have been approved in terms of data protection by the Trust. These providers supply parents / carers with the provider's own privacy notice (via the school / academy) in relation to data protection and, from a safeguarding perspective, they enter into a consent agreement with parents, where the child is engaging with the tutor from the child's home.

School / the academy must ensure that no child engages in such tutoring / interventions / coaching from the child's home if the parents / carers have not signed and returned the consent form to the provider.

- *ABC Teachers*
- *Connex Education Partnership*
- *Teaching Personnel*
- *Learning Academies*
- *Third Space*

Any other third party providers must be approved by the school / academy and by the Trust's Central Team both in terms of safeguarding and data protection.

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' / academies 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 and have been approved for use (see list of approved platforms on Governor Hub) – if in doubt, check with the Trust's 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 Trust's 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, BYOD Policy and 'Live' Teaching (delivered remotely) and Remote Meetings Guidance for parents / carers and pupils;
- staff to watch the Trust's 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

Any meeting / CPD session held virtually should be via Zoom, Microsoft Teams or Google Classrooms and the above guidelines must be adhered to.