



# Remote Learning Policy

To be adhered to in the event of school having to close for face-to-face teaching and move to online learning

**Reviewed: Summer 2025**

**Next Review: Summer 2027**

## **Contents**

1. Aims
2. Roles and responsibilities
3. Who to contact
4. Data protection
5. Safeguarding
6. Monitoring arrangements
7. Links with other policies

## **1. Aims**

This remote learning policy for staff aims to achieve the following:

- Ensure consistency in the school's approach to remote learning
- Set out expectations for all members of the school community with regards to remote learning
- Provide appropriate guidelines for data protection

## **2. Roles and responsibilities**

### **2.1 Teachers**

Teachers would normally be expected to work within the school building. However, if directed by the Headteacher to work from home for any reason, teachers must be available between 8.30am and 3.30pm. If they are unable to work for any reason during this time, for example due to sickness or caring for a dependent, they should report this to the Headteacher.

Teachers are responsible for the following:

#### **Setting work**

- Work should be set for each of a teacher's timetabled classes. Where classes are shared, responsibility for setting the work should be split proportionately.
- The amount of work set should equate to the number of timetabled teaching hours per week.
- The work should be set via Microsoft Class Teams or the website, with any materials needed being attached / linked to the instructions for each task. Work may be varied in nature and can include, but is not exclusive to, note taking, task completion, use of online packages such as, Timetables Rockstars, Oxford Owl etc
- Teachers should coordinate with other teachers to ensure consistency across the year/subject and to make sure students with limited access to devices can still complete the work.

#### **Providing feedback on work**

- Completed work can be uploaded for teachers via Microsoft Class Teams, phase leader group email addresses and the class pages. Quizzes may be self-marked, and teachers can provide comments.
- Feedback can be given in written form on Microsoft Class Teams.

#### **Keeping in touch with students and parents**

- If contacting home via telephone, staff should make contact from school, if in the building at the time. If using personal phones, staff should ensure that personal numbers are withheld.
- Teachers contacting home for pastoral purposes should ensure that any issues are passed on to the appropriate member of staff, where appropriate and notes recorded on CPOMS. (Teaching & Learning issues – refer to class teacher / Key Stage Leader; pastoral issues – refer to Pastoral team; safeguarding issues – refer to DSL immediately.)
- Emails from students / parents should be responded to from a school email address within normal working hours. A response should be sent within one working day of receipt of email; this may take the form of a 'holding email' if necessary.
- Communications to students should only be to the student's Class Teams account.

#### **Attending virtual meetings with staff, parents and students**

- These should only take place within the school's working hours.
- MS Teams must be used for virtual meetings.
- Staff should take care in choosing the location from which they are meeting, ensuring that there is nothing inappropriate in the background and that they will not be disturbed during the meeting by someone who does not work for the school.
- A note of the time of any virtual meeting with students / parents should be made in planning folders on weekly timetables along with any notes from the meeting which are deemed necessary.
- Any concerns arising from a virtual meeting with students / parents should be passed on to the appropriate member of staff and notes recorded on CPOMS. (Teaching & Learning issues – refer to class teacher / Key Stage Leader; pastoral issues – refer to Pastoral team; safeguarding issues – refer to DSL immediately.)

#### **Online teaching**

- Lessons should only take place within the school's working hours and should last no longer than one hour.
- MS Teams must be used for online teaching. No other platform should be used.
- Staff should take care in choosing the location from which they are teaching, ensuring that there is nothing inappropriate in the background and that they will not be disturbed during the lesson by someone who does not work for the school. (The 'Blur Background' function can be used on MS Teams if needed.)
- Notice of the lesson should be posted in Microsoft Class Teams, with the title 'Video lesson for [maths] at [10.00am] on [18th November]', so the students are aware of the time and nature of the lesson. Parents need to be fully aware of the timetable for all children, especially younger children.

- Students may be asked to turn off cameras & microphones for the lesson, unless instructed otherwise by the teacher during the lesson.

## **2.2 Teaching assistants**

Teaching assistants must be available between 8:30am and 3.30pm on their days. If they're unable to work for any reason during this time, for example due to sickness or caring for a dependent, they should report this using the absence procedure.

Teaching Assistants will be supporting their usual Year group.

### **TAs supporting SEND students working at home:**

- Weekly telephone calls to check on well-being and any issues of work completion being set for Home Learning to be made by Teaching Assistants to EHCP students.
- Record of telephone calls to be logged in a file in planning folder. Any concerns arising from a telephone call with students / parents should be passed on to the appropriate member of staff and notes recorded on CPOMS (Teaching & Learning issues – refer to class teacher / Key Stage Leader; pastoral issues – refer to Pastoral team; safeguarding issues – refer to DSL immediately.)
- Teaching Assistants also prepare notes/modified materials for specific needs as required by the teacher.

## **2.3 Phase Leaders**

Alongside their teaching responsibilities, as outlined above, phase leaders are responsible for:

- Monitoring the work set remotely for their phase. (Amount / timing etc)
- Working with teachers in their phase to make sure work set is appropriate and consistent.
- Working with other phase leaders to make sure work set across subjects is appropriate and consistent, and deadlines are being set.
- Alerting teachers to resources they can use to teach their year group.
- Adapting the curriculum as appropriate for remote learning.

## **2.4 Senior leaders**

Alongside any teaching responsibilities, senior leaders are responsible for:

- Coordinating the remote learning approach across the school (Deputy Headteacher and Headteacher will liaise regarding this).
- Monitoring the effectiveness of remote learning, through regular meetings with phase leaders, subject leaders reviewing work set or reaching out for feedback from students and parents.
- Monitoring the security of remote learning systems, including data protection and safeguarding considerations.

## **2.5 Designated safeguarding lead**

The DSL is Mrs Jenny Thomas, Headteacher

The Deputy Safeguarding Leads are:

Mrs Nikki Harvey, Deputy Head Teacher

Mr Dave Kirkpatrick, Assistant Head Teacher

Mrs Karen Sturmey, Learning Mentor

Miss Clare Thornhill, Pastoral HLTA

The Child Protection policy has been reviewed and updated and is available on the school website.

## **2.6 IT staff**

IT staff are responsible for the following:

- Fixing issues with systems used to set and collect work.
- Helping staff and parents with any technical issues they're experiencing.
- Reviewing the security of systems and flagging any data protection breaches to the data protection officer.
- Assisting pupils and parents with accessing the internet or devices.

## **2.7 Pupils and parents**

Staff can expect the following from pupils:

- Be contactable during the school day – although they may not always be in front of a device the entire time.
- Complete work to the deadline set by teachers.
- Seek help if they need it, from teachers or teaching assistants.
- Alert teachers if they're not able to complete work or have issues with access.
- Behave appropriately during online lessons. Inappropriate behaviour during a video lesson will result in the student being removed from the lesson and potentially banned from participating in future online lessons.
- Turn on/off cameras during video lessons and mute microphones as asked by the teacher.

Staff can expect the following from parents:

- Make the school aware if their child is sick or otherwise can't complete work.
- Seek help from the school regarding remote learning, if they need it.

## **2.8 Governors**

The governors are responsible for the following:

- Monitoring the school's approach to providing remote learning to ensure education remains as high quality as possible.
- Ensuring appropriate security policies are in place, for both data protection and safeguarding reasons.

### 3. Who to contact

If staff have any questions or concerns, they should contact the following individuals:

- Issues in setting work – talk to the phase leader.
- Issues with behaviour – talk to the phase leader or pastoral team.
- Issues with IT – talk to IT staff.
- Issues with their own workload or wellbeing – talk to their phase leader.
- Concerns about data protection – talk to Business Manager.
- Concerns about safeguarding – **talk to a DSL immediately.**

### 4. Data protection

**Everyone** in the school has the responsibility of handling protected or sensitive data in a safe and secure manner.

#### Where to get advice

The Information Asset Owners manage and address risks to the information and understand the following:

- what information is held, for how long and for what purpose
- that data can only be used in ways consistent with the purpose/s for which it was obtained, and that data is disclosed only in ways consistent with that purpose
- how information has been amended or added to over time
- who has access to protected data and why

All staff must always follow the GDPR – Data Protection policy – For convenience, a summary of relevant practical steps is included in the sections below.

#### 4.1 Keep data safe and secure

When accessing personal data, all staff members will **keep data safe and secure**:

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

- All paper-based material containing sensitive personal data must be held in lockable storage, whether on or off site. (ALL Staff)
- Dothill School designates the Headteacher, J Thomas and the Network Managers, T&W as the persons with responsibility for the security of IT systems. The school holds a record of all security measures in place.
- The school will ensure that ICT systems are set up so that the existence of protected files is hidden from unauthorised users. Access to protected data will be controlled according to the role of the user.
- All users will use strong passwords which must be changed regularly, every 100 days. User passwords must never be shared.
- Personal data may only be accessed on machines that are securely password protected. Any device that can be used to access data must be locked if left (even for very short periods). (ALL Staff)
- All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.
- Personal data can only be stored on school equipment. Private equipment (ie owned by the users, including personal cloud storage accounts and personal email accounts) must not be used for the storage of personal data. (ALL Staff)
- Ensure that no unauthorised person can access data from computers that are no longer in use or subject to change of use. This will normally require the removal of all storage media from the device and safe disposal of any data stored on that media.
- The school has clear policy and procedures for the automatic backing up, accessing and restoring all data held on school systems, including off-site backups.
- The school has clear policy and procedures for the use of “Cloud Based Storage Systems” and is aware that data held in remote and cloud storage is still required to be protected in line with the Data Protection Act. The school will ensure that it is satisfied with controls put in place by remote / cloud-based data services providers to protect the data.

#### **4.2 Sharing personal data**

Dothill Primary School may need to access personal information, such as email addresses as part of the remote learning system. Such collection of personal data applies to our functions as a school and doesn't require explicit permissions.

While this may be necessary, individual members of staff are reminded that they should not collect and/or share personal data online as part of their 'online teaching and learning' activity. Any data required to carry out online teaching and learning will be collected and managed centrally by the Network Manager.

#### **4.3 Secure transfer of data and access out of school**

Dothill Primary School recognises that personal data may be accessed by users out of school or transferred to the LA or other agencies. In these circumstances:

- Users may not remove or copy sensitive or restricted or protected personal data from the school or authorised premises without permission and only when the criteria (b) and (c), below are met. (ALL Staff)
- When restricted or protected personal data is required by an authorised user from outside the organisation's premises (for example, by a member of staff to work from their home), they should preferably have secure remote access to the management information system or learning platform. (ALL Staff)

NOTE: VPN is available to use via staff laptops.

Direct Remote Access is available to use from all other devices.

- a) If secure remote access is not possible, personal data can only be stored on your "staff laptop". (ALL Staff):
- b) The use of USB stick, CD/DVD or any other removable media is not permissible for the transfer of personal data outside of school.
- c) Users must take particular care that computers (staff laptops) which contain personal data must not be accessed by other users (e.g. family members) when out of school. (ALL Staff)
- d) If staff take home paper-based materials containing personal data (including exercise books, assessments, tests or exam scripts) these documents must NOT be left in a vehicle overnight.
- e) Staff will be made aware of all practical measures to ensure the security of personal data, annually and through 'new staff' induction procedures.
- f) Trainee and associate teachers working and training temporarily at Dothill Primary School will, as part of their induction process, be required to encrypt and password protect any removable media device that they intend to use whilst on placement at Dothill Primary School. At the end of their placement, they must present their removable media device to the IT technician in order to ascertain and ensure all and any personal data has been removed from their device.

Sending information via email is by default not secure just like sending mail in the postal system the mail can be intercepted and read by anyone:

- g) email attachments that contain personal data must be **password protected and encrypted** first before sending them but then providing the recipient a password via **separate** communication channel for example a phone call.

#### 4.4 Data Breaches

What is a personal data breach?



A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Personal data breaches can include the following:

- access by an unauthorised third party
- deliberate or accidental action (or inaction) by a controller or processor
- sending personal data to an incorrect recipient
- computing devices containing personal data being lost or stolen
- alteration of personal data without permission; and
- loss of availability of personal data.

If a member of staff considers that a breach of personal data has occurred, they will inform Julie Thornton (SBM) who will seek advice from school governance and complete sections 1 – 4 of the Personal Data – Breach Record within 24hrs. (ALL Staff)

## **5. Safeguarding**

The Child Protection Policy is reviewed and updated annually – it has been further updated and is available on the school website.

## **6. Monitoring arrangements**

This policy will be reviewed every 12 months (or sooner if deemed necessary). At every review, it will be approved by SLT and the governors.

## **7. Links with other policies**

This policy is linked to the following other policies:

Behaviour policy

Child protection policy

Data protection policy and privacy notices

ICT and internet acceptable use policy

Online safety policy