NORTON CANES HIGH SCHOOL

Remote Learning Policy

Approved by:

Last reviewed on: September 2023

Next review by: September 2024

1. Statement of intent

At Norton Canes High School, we understand the need to continually deliver high quality education, including during periods of remote working. We recognise the importance of maintaining high expectations in all areas of school life and ensuring that all pupils have access to the learning resources and support they need to succeed.

Through the implementation of this policy, we aim to address the key concerns associated with remote working, such as online safety, access to educational resources, data protection, and safeguarding.

This policy aims to:

- Minimise the disruption to pupils' education and the delivery of the curriculum.
- Ensure consistency in the approach to remote learning for pupils who aren't in school
- Set out expectations for all members of the school community with regards to remote learning
- Ensure provision is in place so that all pupils have access to high quality learning resources.
- Protect pupils from the risks associated with using devices connected to the internet.
- Ensure staff, parent, and pupil data remains secure and is not lost or misused.
- Ensure robust safeguarding measures continue to be in effect during the period of remote learning.
- Ensure all pupils have the provision they need to complete their work to the best of their ability, and to remain happy, healthy, and supported during periods of remote learning.

2. Roles and responsibilities

2.1 Teachers

When providing remote learning, teachers must be available between 8:40 and 3:30.

If they are unable to work for any reason during this time, they should report this using the normal absence procedure.

When setting work, it is important to be aware that not all pupils' home environments will support their education. Some may not have access to a device or have an internet connection at home that allows them to learn online, or join in at scheduled lesson times.

Pupils are more likely to have access to mobile phones than laptops or computers, so using formats (like PDFs) that can be viewed on mobile devices can improve access to resources.

With children spending more time online, it's important to consider online safety when planning and designing teaching activities.

When providing remote learning, teachers are responsible for:

- Setting work for all classes that they teach.

  Work should be set according to the timetable and curriculum in place at the time of remote learning to ensure continuity. Work should be set on Satchel One for all years 7 to 11. Sixth Form will be set via Microsoft Teams. Work must be set to appear by the time your timetabled lesson is due to start (you may choose to set the work before this time and choose the date for it to appear Satchel One). Pupils should be set one hour's worth of work. Where possible, this should include a range of activities and not rely entirely on the use of technology to complete. All work must include a recall activity at the start.

  Where possible, it is worth considering adding 'voice-over' onto work so instructions are clear and help students with engagement.

  Some curriculum areas may choose members of staff to set work for a whole year group. This is acceptable as long as agreed in advance and all members of the department are clear on the arrangements.

  After a sequence of lessons, set a summative quiz to assess learning before continuing to new learning.

- Providing feedback on work:

  Pupils will send work to teachers via Satchel One, Microsoft Teams or other online learning platforms such as Dr Frost Maths. Pupils will not send work via email as this does not allow for easy feedback or tracking of work to take place.

  Teachers should provide feedback for all work in the following format via Satchel One or Microsoft Teams:

  - One Kudos point to be awarded for each piece handed in – more may be awarded for effort
  - Quiz scores are sufficient feedback, followed by whole-class feedback on areas of for general improvement.

- Keeping in touch with pupils who aren't in school and their parents:

  Teachers should maintain contact with their pupils via feedback or messages on Show My Homework.

  Form tutors should schedule a weekly live Microsoft Teams session for PSHE/well-being checks

  Teachers will respond to messages and emails during the working hours of 8:45 to 3:30. Staff are to be available online to students during their timetabled lessons.

  Safeguarding concerns should be referred to the safeguarding team by sending an email and logging CPOMS.

  Complaints or concerns shared by parents or pupils that cannot be dealt with by the class teacher should be referred to the curriculum lead or the respective SLT line manager

  If pupils are failing to complete work, parents should be contacted. Before doing so, please check with the safeguarding team in case they are aware of reasons for the non-completion.

- Attending virtual meetings with staff, parents and pupils:

Live sessions on Microsoft Teams for pupils may be delivered. All live sessions must be recorded. All meetings must be set with the control solely with the teacher. Pupils must not be permitted into the lesson until accepted. They must wait in the virtual lobby. Pupils should have their cameras off at all times.

Please also refer to the remote learning protocols policy.

- clothing should be inline with the Staff Code of Dress.
- Be situated in a suitable 'public' living area within the home with an appropriate background.
- Use appropriate language – this includes others in their household.
- Maintain the standard of behaviour expected in school. Pupils who do not follow the behaviour expectations, are to be virtually removed from the lesson.
- Use the necessary equipment and computer programs as intended.
- Not distribute video material without permission.
- Ensure they have a stable connection to avoid disruption to lessons.
- Always remain aware that they are visible.

2.2 Teaching assistants

When assisting with remote learning, teaching assistants must be available between 9:00 and 3:00.

If they're unable to work for any reason during this time, they should report this using the normal absence procedure.

When assisting with remote learning, teaching assistants are responsible for:

- Supporting pupils who aren't in school with learning remotely:
    - Making contact with specified pupils and parents.
    - Liaising with class teachers with any issues

When in school, teaching assistants will be used for First Aid cover and assisting the learning of any identified pupils.

2.3 Curriculum leads

Alongside their teaching responsibilities, curriculum leads are responsible for:

- Considering whether any aspects of the subject curriculum need to change to accommodate remote learning
- Working with teachers teaching their subject remotely to make sure all work set is appropriate and consistent
- Working with other curriculum leads and senior leaders to make sure work set remotely across all subjects is appropriate and consistent, and deadlines are being set an appropriate distance away from each other
- Monitoring the remote work set by teachers in their subject using Satchel One reports and regular contact via email and Microsoft Teams meetings
- Alerting teachers to resources they can use to teach their subject remotely
- Making contact with members of staff they are responsible for once per week.

2.4 Senior leaders

Alongside any teaching responsibilities, senior leaders are responsible for:

- Co-ordinating the remote learning approach across the school (PI)
- Monitoring the effectiveness of remote learning using Satchel One reports and feedback from teachers, pupils and parents (PI)
- Monitoring the security of remote learning systems, including data protection and safeguarding considerations (PO, FA)

2.5 Designated safeguarding lead

The DSL is responsible for:

- Setting up the monitoring system of vulnerable pupils using designated staff for points of contact
- Checking CPOMS and acting on any referrals
- Attending and arranging, where necessary, any safeguarding meetings that occur during the remote learning period.
- Liaising with the ICT technicians to ensure that all technology used for remote learning is suitable for its purpose and will protect pupils online.
- Identifying vulnerable pupils who may be at risk if they are learning remotely.
- Ensuring that child protection plans are enforced while the pupil is learning remotely, and liaising with the headteacher and other organisations to make alternate arrangements for pupils who are at a high risk, where required.
- Identifying the level of support or intervention required while pupils learn remotely and ensuring appropriate measures are in place.
- Liaising with relevant individuals to ensure vulnerable pupils receive the support required during the period of remote working
- Ensuring all safeguarding incidents are adequately recorded and reported.

2.6 SENCO

The SENCO is responsible for:

- Liaising with the ICT technicians to ensure best endeavours are made for technology used for remote learning be accessible to all pupils.
- Ensuring that pupils with EHC plans continue to have their needs met while learning remotely, and liaising with the headteacher and other organisations to make any alternate arrangements for pupils with EHC plans.

2.7 IT Support

IT support are responsible for:

- Fixing issues with systems used to set and collect work that are in the control of NCHS
- Helping staff and parents, where possible, with any technical issues they're experiencing

- Reviewing the security of remote learning systems and flagging any data protection breaches to the data protection officer
- Assisting pupils and parents with accessing the internet or programs

IT support must be contacted using the following email address: ITSupport@nortoncanes-high.staffs.sch.uk.

The school will ensure that all school-owned equipment and technology used for remote learning has suitable anti-virus software installed, can establish secure connections, can recover lost work unless it has been stored locally or on a device not owned by the school, and allows for audio and visual material to be recorded or downloaded, where required.

2.8 Data Protection

The Data Protection Officer is responsible for:

- Overseeing that all school-owned electronic devices used for remote learning have adequate anti-virus software and malware protection.
- Ensuring all staff, parents, and pupils are aware of the data protection principles outlined in the GDPR.
- Ensuring that all computer programs used for remote learning are compliant with the GDPR and the Data Protection Act 2018.
- Overseeing that any ICT equipment used for remote learning is resilient and can efficiently recover lost data unless it has been stored locally or on a device not owned by the school.

2.9 Pupils and parents

Staff can expect pupils learning remotely to:

- Be contactable during the school day – although consider they may not always be in front of a device the entire time
- Complete work to the deadline set by teachers to their best ability and using the Norton Standard (date and title) and submit it via Satchel One. Even if using a different platform, pupils can submit a screenshot of the work completed.
- Maintain a good work ethic and a high quality of work during the period of remote learning.
- Seek help if they need it, from teachers by messaging through Satchel One or by emailing using their school email address
- Alert teachers if they're not able to complete work for any reason
- Hand in work via Satchel One or Microsoft Teams (not email) before the next lesson
- Reporting any technical issues to their teacher as soon as possible.
- Ensuring they have access to remote learning material and notifying a responsible adult if they do not have access.

Pupils are accountable for the completion of their own schoolwork – teaching staff will contact parents via email if their child is not completing their schoolwork or their standard of work has noticeably decreased.

Pupils must adhere to this policy at all times during periods of remote learning.

Staff can expect parents with children learning remotely to:

- Make the school aware if their child is sick or otherwise can't complete work
- Seek help from the school if they need it
- Be respectful when making any complaints or concerns known to staff taking into consideration that staff may be working from home and also supervising their own children

Should students require additional work, parents and pupils can make use of the following online resources:

Oak National Academy: www.thenational.academy

BBC Bitesize: www.bbc.co.uk/bitesize

BBC Daily Lessons: www.bbc.co.uk/bitesize/dailylessons

Parents are responsible for:

- Adhering to this policy at all times during periods of remote learning.
- Ensuring their child is available to learn remotely at the times set out in paragraphs 9.1 and 9.2 of this policy, and that the schoolwork set is completed on time and to the best of their child's ability.
- Reporting any technical issues to the school as soon as possible.
- Ensuring that their child always has access to remote learning material during the times set out in this policy
- Ensuring their child uses the equipment and technology used for remote learning as intended.

If a child is absent from school due to illness or because they are self-isolating, guidance will be provided by school for how students can access work – see appendix 1.

2.10 Governing body

The governing body is responsible for:

- Monitoring the school's approach to providing remote learning to ensure education remains as high quality as possible
- Ensuring that staff are certain that remote learning systems are appropriately secure, for both data protection and safeguarding reasons

3. Resources and Learning materials

3.1. For the purpose of providing remote learning, the school may make use of:

- Digital work booklets
- Digital past and mock exam papers
- Online learning portals
- Educational websites
- Reading tasks
- Live webinars
- Pre-recorded video or audio lessons

3.2. Teachers will review the DfE's list of online education resources and utilise these tools as necessary, in addition to existing resources.

3.3. Reasonable adjustments will be made to ensure that all pupils have access to the resources needed for effective remote learning.

3.4. Lesson plans will be adapted to ensure that the curriculum remains fully accessible via remote learning, where practical – where this is not practical, the school will ensure pupils can catch up on these areas of the curriculum when they return to school.

3.5. Any defects or issues with remote learning resources will be reported as soon as possible to the relevant member of staff.

3.6. Pupils will be required to use their own or family-owned equipment to access remote learning resources, unless the school agrees to provide or loan equipment, e.g. laptops.

3.7. Pupils and parents will be required to maintain the upkeep of any equipment they use to access remote learning resources.

3.8. The arrangements for any 'live' classes will be communicated before the allotted time and kept to a reasonable length of no more than one hour per session.

3.11. The ICT technicians are not responsible for providing technical support for equipment that is not owned by the school.

4. Who to contact

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

- Issues in setting work – Class teacher, Form tutor, Curriculum Lead, Ms Pitt
- Issues with behaviour – Mrs Tuli
- Issues with IT – email IT Support@nortoncanes-high.staffs.sch.uk
- Issues with their own workload or wellbeing – line manager
- Concerns about data protection –data protection officer (Mr Farley)
- Concerns about safeguarding – DSL/DDSL (Miss Powell)

5. Data protection

5.1 Accessing personal data

When accessing personal data for remote learning purposes, all staff members will:

Only access data through the school Remote Desktop Server (RDS) from a secure location and on a private Wi-Fi network and never from a public Wi-Fi location. Care should be taken to end all sessions correctly, closing all connections and logging out.

5.2 Processing personal data

Staff members may need to collect and/or share personal data such as care plans, email addresses, performance results etc. as part of the remote learning system. As long as this processing is necessary for the school's official functions, individuals won't need to give permission for this to happen.

However, staff are reminded to collect and/or share as little personal data as possible online.

5.3 Keeping devices secure

Guidance provided in the School Information Security Policy should be considered.

Password and Access Control

Access to Data stored electronically must be controlled through the use of a Strong Password;

Access to Authorised User accounts must be controlled, as a minimum, through the use of a password, which must not be less than 8 characters in length, use both upper and lower case and include at least one special character. Where a system or service, provides alternative authentication methods, including but not limited to, facial or biometric recognition, the alternative authentication method must be in additional to a password;

Members of Staff must ensure that they have a Strong Password for all Authorised User accounts and the same password not re-used across different types of system;

All Authorised Users should ensure they have a Strong Password for all accounts;

Authorised Users are responsible for keeping their assigned password(s) secure and must ensure their password(s) is neither disclosed to, nor used by, anyone else under any circumstances;

Use of another person's username or password will constitute an Information Security Breach and must be reported in accordance with the procedures set out in this policy or any other relevant policy from time to time in force;

Authorised Users are responsible for ensuring that all School and/or Client Devices used to access Data or other confidential information, are logged off, switched off or otherwise controlled by a Strong Password when unattended or not in use, at all times

Authorised Users with access to the School network or a Client Device which is used for, or in connection with School business is responsible for any actions carried out under their username and password.

Use of Client and Personal Devices

A Client device is considered a piece of hardware or software that allows a user remote access to the schools servers and MIS (Management Information System).

Client Devices used for, or in connection with, School business and in particular for the collection or storing of Personal Data and/or Special Category Personal Data must be kept secure with Strong Passwords (see Definitions).

Client Devices used for, or in connection with, School business must not be left unattended in plain sight at any time, including whilst at home or travelling, and must be protected against loss, damage, misuse or unauthorised access. When not in use, Personal Devices must stored in a secure, lockable location and should never be stored in vehicles, even if locked.

Client Devices used for, or in connection with, School business must not be used to access, view or process Personal Data or Special Category Personal Data in a manner that allows Persons other than the Authorised User to view the Data. See Data Protection Policy.

Personal Devices, including but not limited to, laptops, tablets, telephones, smartphones, desktop computers or other electronic equipment, must not be used to store or transmit Data. Where a Member of

Staff believes there is a legitimate need to process Special Category Personal Data using a Client Device, the Member of Staff should contact their Line Manager with a business case for the provision of a Client Device, who shall evaluate the business case for such request.

Client Devices used for, or in connection with, School business must be updated with the manufacturer's software and other updates regularly when updates become available, and where supported have antivirus software installed and regularly updated.

Client Devices used to store Personal Data or Special Category Personal Data must be encrypted.

Client Devices issued to a Member of Staff for or in connection with, School business by the School must only be used by School Members of Staff. At no time shall any other User, including but not limited to, family members, friends, employee from another organisation, be permitted to use the device.

If a Client Device used for, or in connection with School business it lost or stolen, the loss/theft should be reported to Data Protection Administrator and Network Manager (a.farley@nortoncanes-high.staffs.sch.uk) as soon as possible and in any event within 24 hours of the loss/theft occurring. Where possible the Client Device should be remotely accessed and the information erased.

Removable Media

Removable Media storing Data must only be used as a last resort, when all other options have been considered, including the need to store or process the data. All Data must secure network service is not available.

Only Removable Media that has been encrypted should be used for the storing of Data.

Removable Media should not be used for the storing of Personal Data, Special Category or Sensitive Data unless the device is capable of and has been encrypted.

Removable Media must be stored securely.

If Removable Media used for, or in connection with School business is lost or stolen, the loss/theft should be reported to Data Protection Administrator and Network Manager immediately. Where possible the Personal Device should be remotely accessed and the information erased.

Cloud Computing

Only cloud computing networks or services e.g. Office 365, including Social Media commissioned by the School, or expressly authorised by the Data Protection Administrator, may be used to store and send information concerning or relating to School business. The use of personal cloud storage solutions (Skydrive, G-Drive etc.) for the transfer of School information is expressly forbidden. For this express purpose all staff have a school One Drive Business account.

Personal Data, Special Category Personal, confidential and sensitive information, whether on the School network or a Client Device must not be stored on a cloud computing network or service not commissioned by the School, or expressly authorised by the Data Protection Officer.

If Data or other information concerning or relating to School business is to be stored in or on a cloud network, the School will take all reasonable steps to find out in which country the Data or other information is being stored, and to ensure that appropriate measures are in place in relation to any Data transferred outside of the EEA.

If the School receives notification that Data in respect of School business has been corrupted, lost or otherwise compromised while stored on a cloud network, the School should ascertain whether any or all of the information stored in the cloud can be recovered and if this is possible restore that information;

Any corruption, loss or compromise of information held on a cloud network should be recorded in the risk register and if appropriate reported via the reporting procedure set out in the Data Protection Policy.

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring the hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing antivirus and anti-spyware software
- Keeping operating systems up to date – always install the latest updates

Staff should also read and adhere to the following policies:

- The Information Security Policy
- The Data Protection Policy
- Video conferencing protocols for staff and students

6. Safeguarding

6.1. This section of the policy will be enacted in conjunction with the school's Child Protection and Safeguarding Policy

6.2. The DSL will identify 'vulnerable' pupils (pupils who are deemed to be vulnerable or are at risk of harm) via risk assessment prior to the period of remote learning.

6.3. The DSL will arrange for regular contact to be made with vulnerable pupils, prior to the period of remote learning.

6.4. Phone calls made to vulnerable pupils will be made using school phones where possible and if not, staff will be asked to remove their caller ID.

6.5. The DSL will arrange for regular contact with vulnerable pupils three times per week.

6.6. All contact with vulnerable pupils will be recorded using the agreed method and suitably stored in line with the Records Management Policy.

6.7. The DSL will keep in contact with vulnerable pupils' social workers or other care professionals during the period of remote working, as required.

6.8. Vulnerable pupils will be provided with a means of contacting the DSL, their deputy, or any other relevant member of staff – this arrangement will be set up by the DSL prior to the period of remote learning.

6.9. The DSL will meet (in person or remotely) with the relevant members of staff once per week to discuss new and current safeguarding arrangements for vulnerable pupils learning remotely.

6.10. All members of staff will report any safeguarding concerns to the DSL immediately.

5.11. Pupils and their parents will be encouraged to contact the DSL if they wish to report safeguarding concerns, e.g. regarding harmful or upsetting content or incidents of online bullying. The school will also signpost families to the practical support that is available for reporting these concerns.

7. BTEC specific guidance

The school will:

• Ensure that teaching/delivery/assessment staff continue to support blended learning when learners are working remotely using the methods outlined in section 2

• Ensure there is a process to manage feedback on assignments, questions are constructively answered, and feedback is provided in a timely manner

• Ensure the setting of assignments is undertaken and that deadlines are clear

• Ensure that when learners submit work measures are taken to ensure the work is authentic and has been completed by the learner

• Maintain and store securely all assessment and internal verification records in accordance with Pearson Centre Agreement.

8. Links with other policies

This policy is linked to our:

- Behaviour policy
- Child protection policy
- Data protection policy and privacy notices
- Home-school agreement
- ICT and internet acceptable use policy
- Online safety policy
- The Information Security Policy
- Video conferencing protocols for staff and students

Appendix 1: Guide for pupils who are absent from school

If you child is absent from school, we would expect them to keep up with their learning so that they do not fall behind in their studies. Unless your child is too ill to do so, they should check Microsoft Teams and Satchel One daily to see what learning has taken place in class and what homework has been set.

Teachers will upload their materials to Microsoft Teams after the lesson has been taught and will continue to set home learning on Satchel One in the usual way.

How to access Microsoft Teams

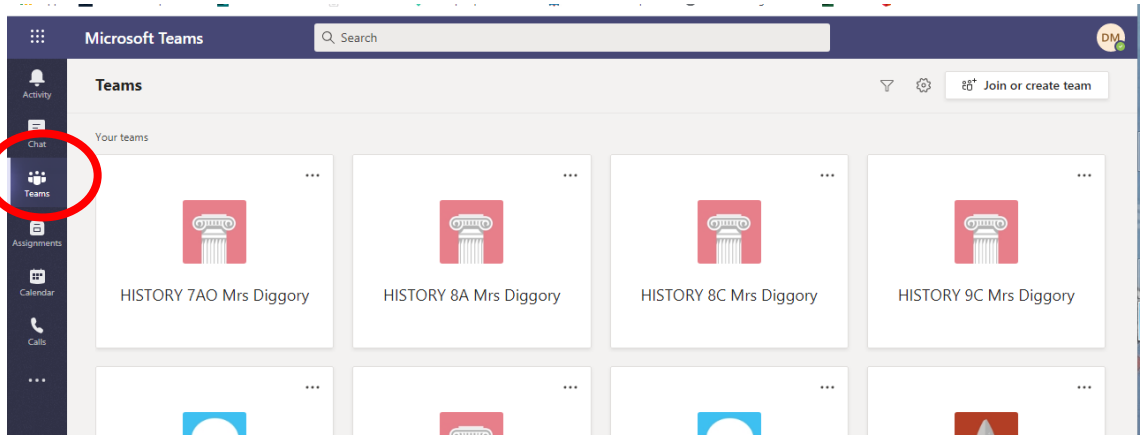
This website page is useful for logging on to Teams and for finding assignments etc:

https://www.nortoncaneshighschool.co.uk/wp-content/uploads/2020/05/Microsoft-Teams-student-guide.pdf

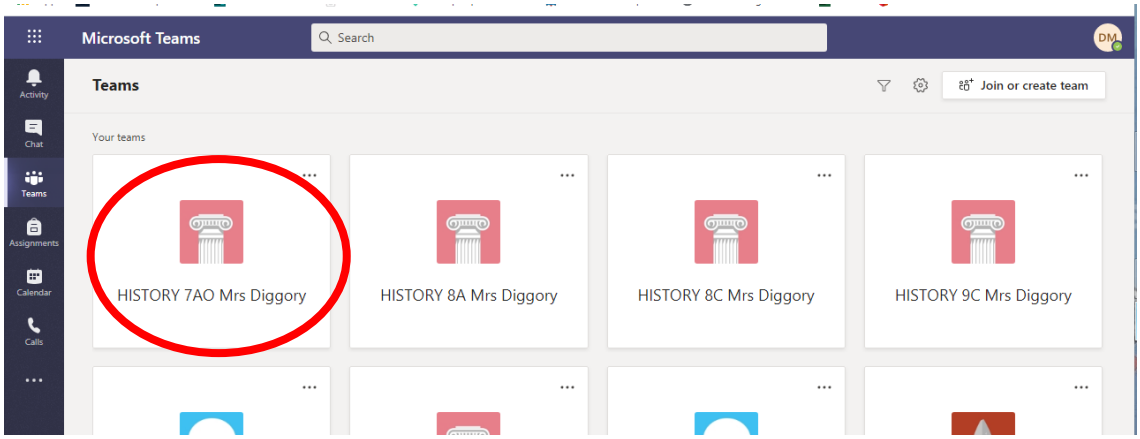
To access class materials, pupils should do the following:

Go to Microsoft Teams

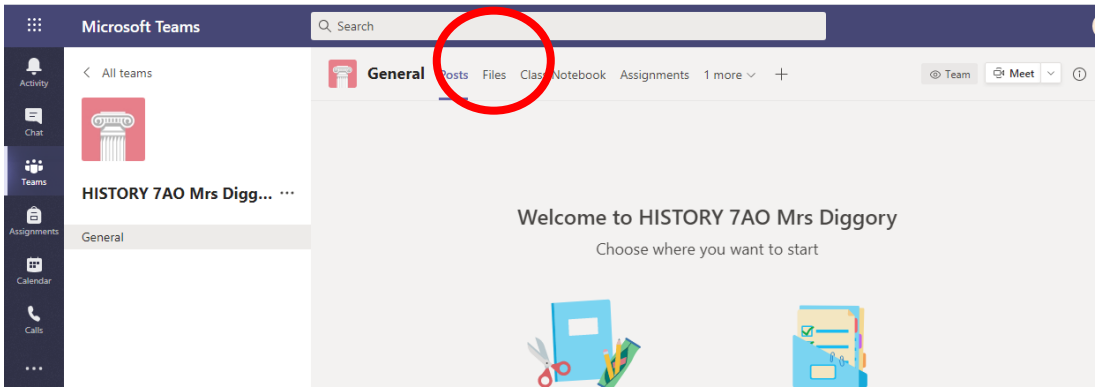
Click on Teams on the left hand side to find the teams they are allocated to



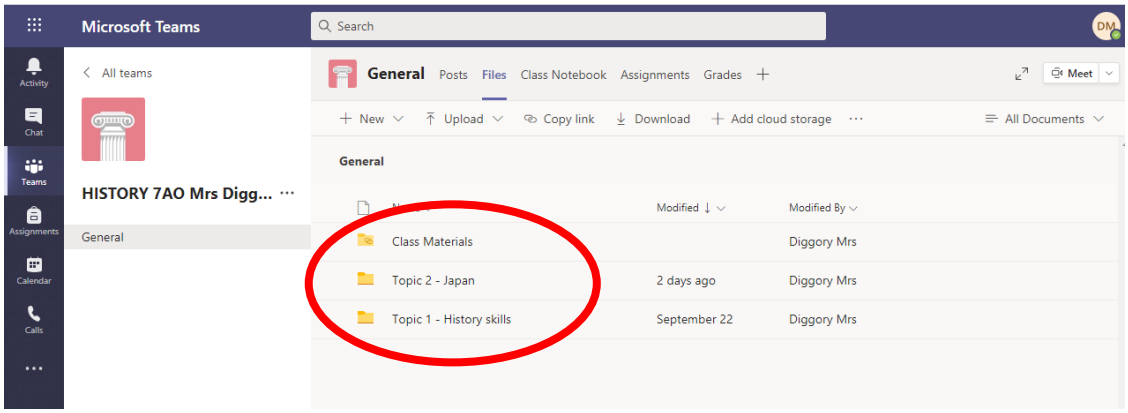
Click on the subject group



Click on the files tab at the top of the section

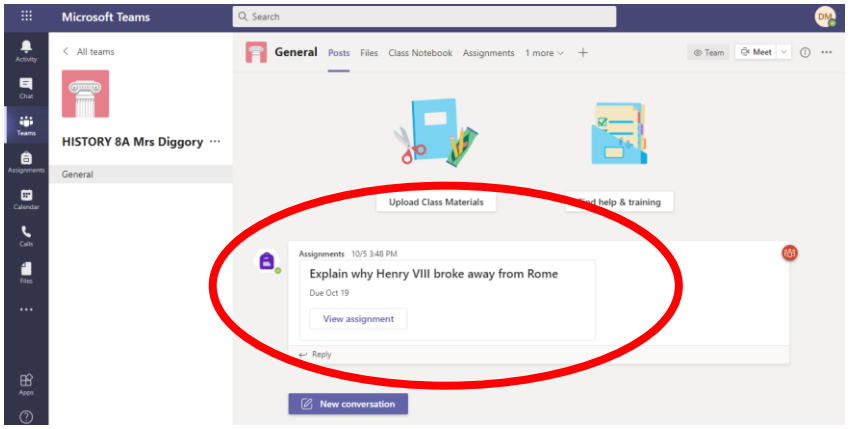


Students will find their lesson on that page or may need to click into the class materials folder.



They can then view any materials that the teacher has shared with the group. Students should attempt any tasks from the lesson and submit them via Satchel One or Microsoft Teams.

Any home learning assignments that have been set will appear on the group home page



If students have questions about their work, they should direct them to the class teacher via email using Microsoft Outlook as part of the Office 365 package.