The John Fisher School
ICT Policy for Staff

Responsible: Governors' Resources Committee

Next Review Date: June 2021

Nurturing young Catholic gentlemen
Aspiring for Academic, Cultural & Sporting Excellence

Introduction

All The John Fisher School's information communication technology (ICT) facilities and information resources remain the property of The John Fisher School and not of particular individuals, teams or departments. By following this policy, read in conjunction with the School's ICT Acceptable Use Policy (http://fluencycontent2-schoolwebsite.netdna-ssl.com/FileCluster/TheJohnFisherSchool/MainFolder/GDPR/ICT-Acceptable-Use-Policy.pdf) and Child Protection and Safeguarding Policy (http://fluencycontent2-schoolwebsite.netdna-ssl.com/FileCluster/TheJohnFisherSchool/MainFolder/our-school/policies/Child-Protection-and-Safeguarding-Policy.pdf) we will help ensure that ICT facilities are used:

- legally;
- securely;
- without undermining The John Fisher School;
- effectively;
- in a spirit of co-operation, trust and consideration for others;
- so that they remain available.

This policy relates to all ICT facilities and services provided by The John Fisher School, although special emphasis is placed on email and the internet. All employees, and any other users of our IT are expected to adhere to the policy.

1. Disciplinary measures

1.1. Deliberate (intentional) and serious (refer particularly to sections 3.2, 4.3 and 8.1.1.5) breach of the policy statements in this section may lead to The John Fisher School taking disciplinary measures in accordance with the relevant disciplinary policy. The John Fisher School accepts that ICT – especially the internet and email system – is a valuable business tool. However, misuse of this facility can have a negative impact upon staff productivity and the reputation of the school.

1.2. In addition, all of the school's phone, internet and email related resources are provided for business purposes. Therefore, the school maintains the right to monitor the volume of internet and network traffic, together with the email systems. The specific content of any transactions will not be monitored unless there is a suspicion of improper use.

2. Security

2.1. As a user of The John Fisher School's equipment and services, you are responsible for your activity.

2.2. Do not disclose personal system passwords or other security details to other staff, or external agents, and do not use anyone else's log-in; this compromises the security of The John Fisher School. If someone else gets to know your password, ensure that you change it or get the IT department to help you.

2.3. If you intend to leave your PC or workstation unattended for any reason, you should lock the screen to prevent unauthorised access. If you fail to do this, you will be

responsible for any misuse of it while you are away. Logging off is especially important where students have access to the screen in your absence.

2.4. Any pen drives or other storage devices used on The John Fisher School's network should be secure. Please see paragraph 7 for more detail.

2.5. Do not attempt to gain unauthorised access to information or facilities. The Computer Misuse Act 1990 makes it a criminal offence to obtain unauthorised access to any computer (including workstations and PCs) or to modify its contents. If you do not have access to information or resources you feel you need, contact the IT department.

3. Use of Email

3.1. When to use email:

3.1.1. Use email in preference to paper to reach people quickly (saving time on photocopying / distribution) and to help reduce paper use.

3.1.2. Use the phone for urgent messages (email is a good backup in such instances). Use of email by staff at The John Fisher School is permitted and encouraged where such use supports the goals and objectives of The John Fisher School.

3.1.3. However, The John Fisher School has a policy for the use of email whereby staff and volunteers must ensure that they:

3.1.3.1. comply with current legislation;

3.1.3.2. use email in an acceptable way;

3.1.3.3. do not create unnecessary business risk to The John Fisher School by their misuse of the internet.

3.2. Unacceptable behaviour:

3.2.1. Sending confidential information to external locations without appropriate safeguards in place. See paragraph 5 of this document for more details.

3.2.2. Viewing, distributing, disseminating or storing images, text or materials that might be considered indecent, pornographic, obscene or illegal.

3.2.3. Viewing, distributing, disseminating or storing images, text or materials that might be considered discriminatory, offensive or abusive, in that the context is a personal attack, sexist or racist, or might be considered as harassment or bullying.

3.2.4. Using copyrighted information in a way that violates the copyright.

3.2.5. Breaking into The John Fisher School's or another organisation's system, or unauthorised use of a password / mailbox.

3.2.6. Broadcasting unsolicited and/or derogatory personal views on social, political, religious, school or other non-business related matters including views that allow, staff or the school to be identified.

3.2.7. Transmitting unsolicited commercial or advertising material.

3.2.8. Undertaking deliberate activities that waste staff effort or networked resources.

3.2.9. Deliberately or recklessly introducing any form of computer virus or malware into the School network.

3.3. Confidentiality

3.3.1. Always exercise caution when committing confidential information to email since the confidentiality of such material cannot be guaranteed. The General Data Protection Regulations (2018) include substantial fines for breaches of personal data – refer to the school's Data Protection and Freedom of Information Policy (http://fluencycontent2-schoolwebsite.netdna-ssl.com/FileCluster/TheJohnFisherSchool/MainFolder/GDPR/Data-Protection-and-Freedom-of-Information-Policy.pdf) and Data Breach Policy (http://fluencycontent2-schoolwebsite.netdna-ssl.com/FileCluster/TheJohnFisherSchool/MainFolder/GDPR/Data-Breach-Policy.pdf). The John Fisher School reserves the right to monitor electronic communications in accordance with applicable laws and policies. The right to monitor communications includes messages sent or received by system users (staff and temporary staff) within and outside the system as well as deleted messages. See paragraph 5 for more detail.

3.4. General points on email use

3.4.1. When publishing or transmitting information externally be aware that you are representing The John Fisher School and could be seen as speaking on The John Fisher School's behalf. Make it clear when opinions are personal. If in doubt, consult your line manager;

3.4.2. Check your inbox at regular intervals during the working day. Keep your inbox fairly empty so that it just contains items requiring your action. Try to decide what to do with each email as you read it (e.g. delete it, reply to it, save the whole email in a folder, or extract just the useful information and save it somewhere logical);

3.4.3. Keep electronic files of electronic correspondence, only retaining what you need to. Do not print it off and keep paper files unless absolutely necessary;

3.4.4. Treat others with respect and in a way in which you would expect to be treated yourself (e.g. do not send unconstructive feedback, argue, or invite colleagues to make public their displeasure at the actions / decisions of a colleague);

3.4.5. Do not forward emails warning about viruses (they are invariably hoaxes and the IT department will probably already be aware of genuine viruses – if in doubt, contact them for advice);

3.4.6. Do not open an email unless you have a reasonably good expectation of what it contains, and do not download files unless they are from a trusted source. For example, do open **report.doc** from a colleague you know but do not open

explore.zip sent from an address you have never heard of, however tempting. Alert the IT department if you are sent anything like this unexpectedly; this is one of the most effective means of The John Fisher School protecting itself against email virus attacks.

3.5. Email signatures

3.5.1. Keep these short and include your name, title, phone number(s) and website address.

4. Use of the Internet

4.1. Use of the internet by staff is permitted and encouraged where such use supports the goals and objectives of the school.

4.2. However, when using the Internet, staff must ensure that they:

4.2.1. comply with current legislation;

4.2.2. use the internet in an acceptable way;

4.2.3. do not create unnecessary business risk to the school by their misuse of the internet.

4.3. Unacceptable behaviour

4.3.1. In particular, the following is deemed unacceptable use or behaviour by staff (this list is non-exhaustive):

4.3.1.1. Visiting internet sites that contain obscene, hateful, pornographic or other illegal material;

4.3.1.2. Using the computer to perpetrate any form of fraud, or software, film or music piracy;

4.3.1.3. Using the internet to send offensive or harassing material to other users;

4.3.1.4. Downloading commercial software or any copyrighted materials belonging to third parties, unless this download is covered or permitted under a commercial agreement or other such licence;

4.3.1.5. Hacking into unauthorised areas;

4.3.1.6. Creating or transmitting defamatory material;

4.3.1.7. Undertaking deliberate activities that waste employees effort or networked resources;

4.3.1.8. Deliberately or recklessly introducing any form of computer virus into The John Fisher School's network.

4.4. Chat rooms / instant messaging (IM)

4.4.1. The use of chat rooms and instant messaging is permitted for business use only.

4.5. Obscenities / pornography

4.5.1. Do not write, publish, look for, bookmark, access or download material that might be regarded as obscene or pornographic.

4.6. Copyright

4.6.1. Take care to use software legally and in accordance with both the letter and spirit of relevant licensing and copyright agreements. Copying software for use outside these agreements is illegal and may result in criminal charges.

4.6.2. Be aware of copyright law when using content you have found on other organisations' websites. The law is the same as it is for printed materials.

5. Confidentiality

5.1. If you are dealing with personal, sensitive and / or confidential information, then you must ensure that extra care is taken to protect the information.

5.2. If sending personal, sensitive and / or confidential information via email, then the following protocols should be used. If there is any doubt as to the information being sent or the appropriate level of protection required, please check with the IT department.

5.2.1. Personal, sensitive and / or confidential information should be contained in an attachment;

5.2.2. In appropriate cases the attachment should be encrypted, and / or password protected;

5.2.3. Any password or key must be sent separately;

5.2.4. Before sending the email, verify the recipient by checking the address, and if appropriate, telephoning the recipient to check and inform them that the email will be sent;

5.2.5. Do not refer to the information in the subject of the email.

6. The John Fisher School's network

6.1. Keep master copies of important data on The John Fisher School's network server and not solely on your PC's local C: Drive or portable disks. Not storing data on The John Fisher School's network server means it will not be backed up and is therefore at risk.

6.2. Ask for advice from the IT department if you need to store, transmit or handle large quantities of data, particularly images or audio and video. These large files use up disk space very quickly and can bring the network to a standstill.

6.3. Be considerate about storing personal (non-The John Fisher School) files on The John Fisher School's network.

6.4. Do not copy files that are accessible centrally into your personal directory unless you have good reason (i.e. you intend to amend them or you need to reference them and the central copies are to be changed or deleted) since this uses up disk space unnecessarily.

7. Removable media

7.1. If storing or transferring personal, sensitive, confidential or classified information using removable media you must first contact your line manager for permission, but

7.1.1. Always consider if an alternative solution already exists;

7.1.2. Only use recommended removable media;

7.1.3. Consider encrypting and password protecting;

7.1.4. Store all removable media securely;

7.1.5. Removable media must be disposed of securely by the IT department.

8. Personal use of ICT facilities

8.1. Social media

For the purposes of this policy, social media websites are web-based and mobile technologies which allow parties to communicate instantly with each other or to share data in a public forum. They include websites such as Facebook, Twitter, Google+ and LinkedIn. They also cover blogs and image sharing websites such as YouTube and Flickr. This is not an exhaustive list and you should be aware that this is a constantly changing area.

8.1.1. Use of Social Media at work

8.1.1.1. Staff and volunteers are permitted to make reasonable and appropriate use of social media websites from The John Fisher School's IT equipment. You should ensure that usage is not excessive and does not interfere with work duties. Use should be restricted to your non-working hours, unless this forms part of your work responsibilities.

8.1.1.2. Access to particular social media websites may be withdrawn in the case of misuse.

8.1.1.3. Inappropriate comments on social media websites can cause damage to the reputation of the school if a person is recognised as being a member of staff. It is, therefore, imperative that you are respectful of the school's service as a whole including parents/carers, students, colleagues and partner organisations.

8.1.1.4. Staff should not give the impression that they are representing, giving opinions or otherwise making statements on behalf of The John Fisher School unless appropriately authorised to do so. Personal opinions must be acknowledged as such, and should not be represented in any way that might

make them appear to be those of the School. Where appropriate, an explicit disclaimer should be included, for example: '*These statements and opinions are my own and not those of The John Fisher School.'*

8.1.1.5. Any communications that staff make in a personal capacity must not:

8.1.1.5.1. bring The John Fisher School into disrepute, for example by criticising parents/carers, students, colleagues and partner organisations;

8.1.1.5.2. breach The John Fisher School's policy on confidentiality or any other relevant policy;

8.1.1.5.3. breach copyright, for example by using someone else's images or written content without permission;

8.1.1.5.4. do anything which might be viewed as discriminatory against, or harassment towards, any individual, for example, by making offensive or derogatory comments relating to: age, disability, gender reassignment, race, religion or belief, sex, or sexual orientation;

8.1.1.5.5. use social media to bully another individual;

8.1.1.5.6. post images that are discriminatory or offensive (or links to such content).

8.1.2. The John Fisher School maintains the right to monitor usage where there is suspicion of improper use.

8.2. Other personal use

8.2.1. Use of facilities for leisure or personal purposes (e.g. sending and receiving personal email, personal phone calls and browsing the internet) is permitted so long as such use does not:

8.2.1.1. incur specific expenditure for The John Fisher School;

8.2.1.2. impact on the performance of your job or role (this is a matter between each member of staff and their line manager);

8.2.1.3. break the law;

8.2.1.4. bring The John Fisher School into disrepute;

8.2.1.5. detrimentally affect the network performance by using large amounts of bandwidth (for instance by downloading / streaming of music or videos);

8.2.1.6. impact on the availability of resources needed (physical or network) for school use.

8.2.2. Any information contained within The John Fisher School in any form is for use by staff for the duration of their period of work and should not be used in any way other than for proper school purposes, or transferred into any other format (e.g. loaded onto a memory stick / pen drive), unless necessary for school use, and with prior agreement by a line manager.

9. Portable and Mobile ICT Equipment

9.1. This section covers items such as laptops, mobile devices and removable data storage devices. Please refer to paragraph 7 of this document when considering storing or transferring personal or sensitive data.

9.2. Use of any portable and mobile ICT equipment must be authorised by line managers before use.

9.3. All activities carried out on The John Fisher School's systems and hardware will be monitored in accordance with the general policy.

9.4. Staff must ensure that all data belonging to The John Fisher School is stored on The John Fisher School's network and not kept solely on a laptop. Any equipment where personal data is likely to be stored must be encrypted.

9.5. Equipment must be kept physically secure in accordance with this policy to be covered for insurance purposes. When travelling by car, best practice is to place the laptop in the boot of the car before starting your journey.

9.6. Synchronise all locally stored data, including diary entries, with the central organisation network server on a frequent basis.

9.7. Ensure portable and mobile ICT equipment is made available as necessary for anti-virus updates and software installations, patches or upgrades.

9.8. The installation of any applications or software packages must be authorised by the IT department, fully licensed and only carried out by the IT department.

9.9. In areas where there are students present, portable or mobile ICT equipment must not be left unattended and, wherever possible, must be kept out of sight.

9.10. Portable equipment must be transported in a protective case if one is supplied.

10. Remote Access

10.1. If remote access is required, you must contact the IT department to set this up.

10.2. You are responsible for all activity via your remote access facility.

10.3. Laptops and mobile devices must have appropriate access protection, i.e. passwords and encryption, and must not be left unattended in public places.

10.4 To prevent unauthorised access to The John Fisher School's systems, keep all dial-up access information such as telephone numbers, logon IDs and PINs confidential and do not disclose them to anyone.

10.5. Select PINs that are not easily guessed, e.g. do not use your house or telephone number and do not choose consecutive or repeated numbers.

10.6. Avoid writing down or otherwise recording any network access information where possible. Any information that is written down must be kept in a secure place and disguised so that no other person is able to identify what it is.

10.7. Protect The John Fisher School's information and data at all times, including any printed material produced while using the remote access facility. Take particular care when access is from a non-School environment.

10.8. Users of laptops and mobile devices are advised to check their car and home insurance policies for the level of cover in the event of equipment being stolen or damaged. Appropriate precautions should be taken to minimise risk of theft or damage.

10.9. Care should be taken when working on laptops in public places (e.g. trains) that any personal data is not visible to other people.

11. Electronic monitoring

11.1 You may find that you have access to electronic information about the activity of colleagues. Any such information must not be used by unauthorised individuals to monitor the activity of individual staff in any way (e.g. to monitor their working activity, working time, files accessed, internet sites accessed, reading of their email or private files, etc.) without their prior knowledge. Exceptions are:

11.1.1 In the case of a specific allegation of misconduct, when the Headteacher can authorise accessing of such information when investigating the allegation;

11.1.2 When the IT department cannot avoid accessing such information while fixing a problem, but this will only be carried out with the consent of the individual concerned.

12. Online purchasing

12.1 Staff are discouraged from ordering online using personal details.
12.2 Any users who place and pay for orders online using personal details do so at their own risk and The John Fisher School accepts no liability if details are fraudulently obtained whilst the user is using The John Fisher School's equipment.

13. Care of equipment

13.1 Do not rearrange the way in which equipment is plugged in (computers, power supplies, phones, network cabling, modems etc.) without first contacting the IT department.

14. Agreement

All staff, contractors or temporary employees who have been granted the right to use The John Fisher School's ICT systems are required to have read and understood.

APPENDIX

Broadcasts in Teaching and Learning (live & recorded) – Safeguarding Issues to Consider

IMPORTANT CONSIDERATIONS

We need to remember that not every family is able to afford the required technology and even if they do, there may not be enough to go round the siblings. Families living in poor housing conditions may have no broadband. The gap between the haves and the have-not's will be noticeable with remote learning. It is likely that children will be using the internet more than ever in an enforced school closure or period of self-isolation, so safer internet messages are particularly important.

REMOTE TEACHING AND LEARNING POLICY - SAFEGUARDING PERSPECTIVE

- The remote learning platform is Show My Homework, please use only your school email to respond to any work issues or any contact from parents/carers or students. This should be done through Edulink where possible.

- Do not contact parents/carers and students on your own mobile phone or landline. If you have been given a school phone, please feel free to use it. You can also use the 141 facility.

- Staff registering for any software/platforms must do so with their school email address.

- Teachers should take into account adaptations to home learning for students with SEND or on the Gifted and Talented register and ensure that they are able to access the work at home and that there are appropriate expectations of the work they will produce.

REPORTING CONCERNS

If you have any safeguarding concerns with student's or parents/carers communication, please enter on My Concern.

FOR NON-INTERACTIVE REMOTE LEARNING (INC BORAODCOAST or PODCAST)

Non Interactive Broadcasts and podcasts will be recordings, so please ensure that:

- You are professionally dressed.
- You are in an appropriate location when recording (neutral background where possible).
- All non-interactive lessons are shared through Show My Homework.

REMOTE LEARNING (Via 'Zoom' Meetings)

This not an expectation, if you choose to deliver some element of live remote learning please stick to the following:

- 'Zoom' meetings to be used only with Year 12 classes.
- Parents/carers to be informed via Edulink of any "live" session you wish to conduct.
- Meetings are to be scheduled as per school timetabled lessons to avoid clashes or during 'core time'.
- Details of the meetings are to be shared through Show My Homework.
- Please consider whether video is necessary as audio will suffice in most cases.
- Staff and students must wear suitable clothing, as should anyone else in the household.
- Any computers used must be in appropriate areas, not in bedrooms, and where possible be against a neutral background.
- 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.
- The live class should be recorded and backed up elsewhere, so that if any issues were to arise, the video can be reviewed (Zoom has this facility).
- Contact your line manager if you are going to use Zoom meetings with any of your classes.
- If you are concerned about privacy issue or safeguarding matters, please do not use live communication.

STUDENTS

- You will be notified of live lessons via Show My Homework.
- If invited to join a video conversation / lesson the student must be suitably dressed and in a communal living area.
- You are to conduct yourself as you would in the classroom.

- Video should only be used if required by the lesson.

PARENTS/CARERS

- Staff will be contacting parents/carers to notify you of any live session scheduled. if you have any issues please contact the staff member prior to the session.
- **Parent/Carer involvement during video sessions:**
  by bringing staff instruction into the home, the lessons can feel different. The same rules of communication apply as if this were a regularly taught lesson meaning that the interaction in these lessons is between the teacher and the students alone.
- Size of groups for home learning: one to one video sessions with student are not allowed.
- This opens staff up to a high level of potential risk.
- The minimum group size for a video session would therefore need to be 3.

Distance Learning

Zoom is one of the most popular online learning options available. It allows you to start or join face to face video calls with up to 100 people. All you need to sign up for Zoom is a valid email address. Download the mobile or desktop app, agree to the privacy policy and the terms and conditions and you're all good to go.

As a school, we are not permitting Zoom to be used to conduct live video lessons with Years 7-11. However, if you wish to use Zoom for Year 12 lessons with smaller manageable numbers, please follow the instructions below on how to set this up. As always, safeguarding is paramount - please follow the advice sent out by Mr Mawer.

Signing up and logging in:

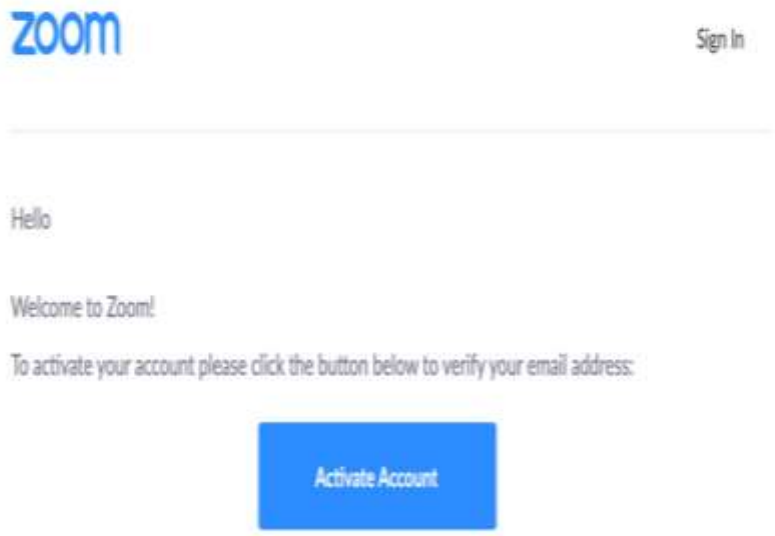
1. How to Sign Up for the First Time

    1. Start by going to zoom.us.

    2. On the top right corner, click on the blue "Sign Up, It's Free" button.

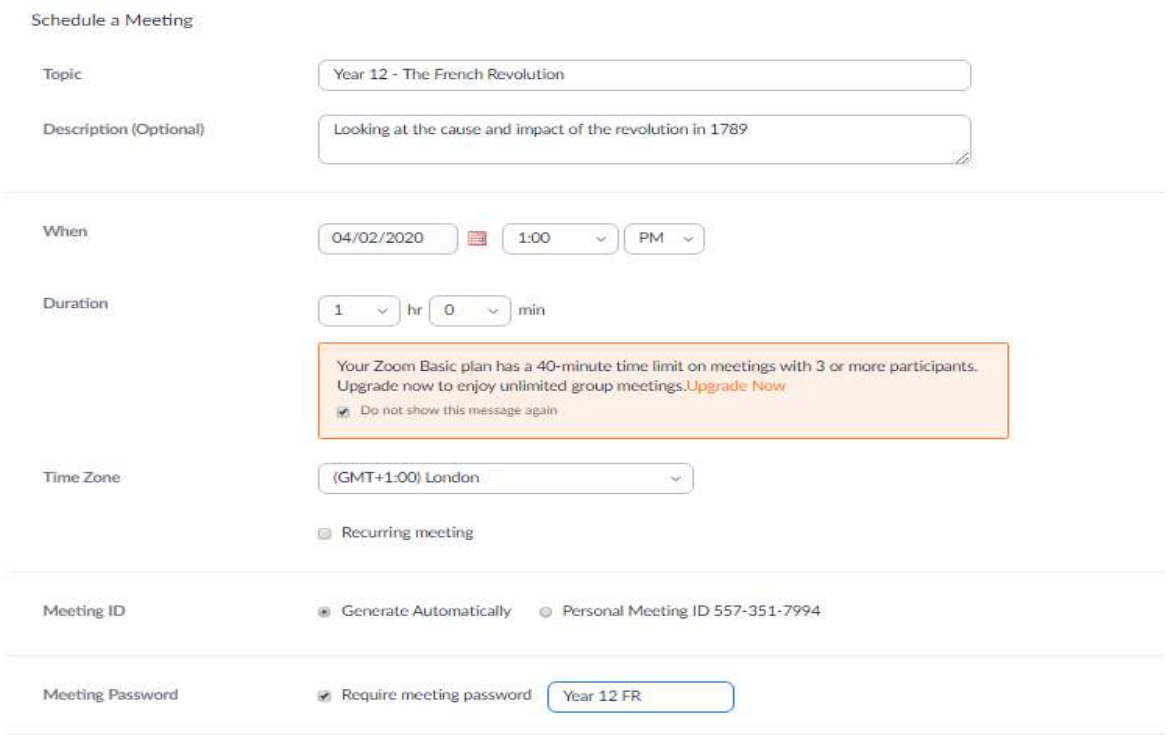
    3. Enter your school email address and click "Sign Up".

4. You'll receive an email from Zoom to activate. Go to your email and click Activate Account.



5. You'll be redirected to fill in your first name, last name, and create a password.

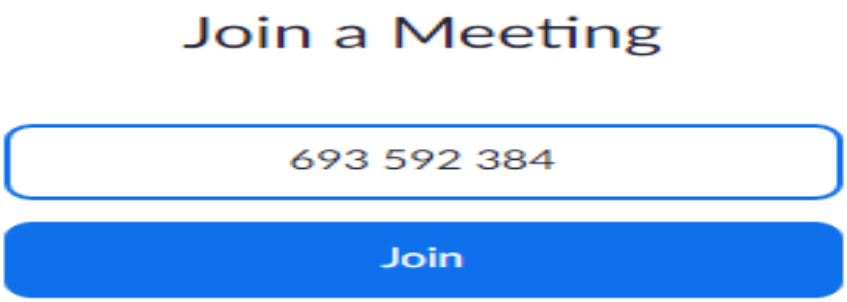
Scheduling a meeting:

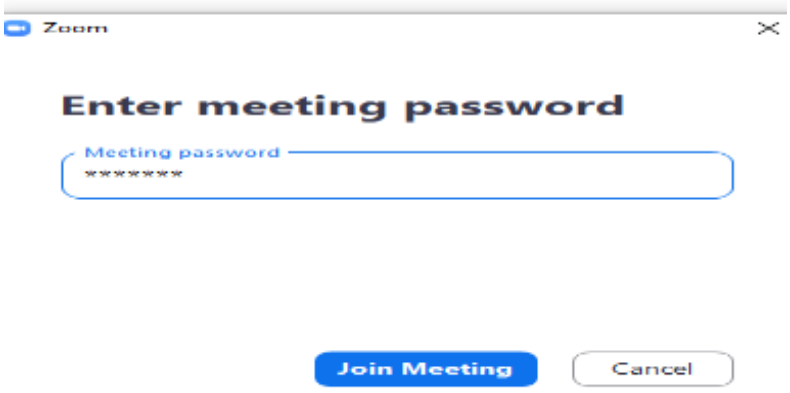


Meeting ID/ Password:

The URL, meeting ID and Pin generated to join the meeting should be shared through Show My Homework. This avoids staff having to have complete student email lists for the class.

Joining a meeting:





The link below is also brief guide on how to set up use Zoom for classes

https://www.youtube.com/watch?v=9guqRELB4dg