



Petersfield E-Safety Policy 2024

Version	Update
Policy Type	Standards
Discussed by staff	Sept 2024
Approved by the Headteachers	Sept 2024
Adopted by the FGB	18 th September 2024
Next Review	2025

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, at Petersfield we need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

E-safety involves pupils, staff, governors and parents making best use of technology, information, training and this policy to create and maintain a safe online and ICT environment for Petersfield School.

"As in any other area of life, children and young people are vulnerable and may expose themselves to danger - knowingly or unknowingly - when using the Internet and other digital technologies. Indeed, some young people may find themselves involved in activities which are inappropriate or possibly illegal.

"To ignore e-safety issues when implementing the requirements of Every Child Matters could ultimately lead to significant gaps in child protection policies, leaving children and young people vulnerable."

From: Safeguarding Children in a Digital World. BECTA 2006

Our E-Safety Policy has been written following government guidance, it has been agreed by pupils, staff, senior management and approved by governors.

- The school's E-safety Lead is Mr Carter.
- The E-Safety Governor is Tanya Brown
- The E-Safety Policy and its implementation shall be reviewed annually.

Roles and Responsibilities

Governors:

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. The role of the E-Safety Governor will include:

- Regular meetings with the E-Safety Lead.
- Regular monitoring of e-safety incident logs.
- Reporting to the Standards Committee.

Headteachers and Senior Leaders:

- The Headteachers are responsible for ensuring the safety (including E-safety) of members of the school community, though the day-to-day responsibility for E-safety will be delegated to the E-Safety Lead.
- The Headteachers/Senior Leaders are responsible for ensuring that the E-safety Lead and other relevant staff receive suitable CPD to enable them to carry out their E-safety roles and to train other colleagues, as relevant.
- The Headteachers/Senior Leaders will ensure that there is a system in place to allow for monitoring and support of teachers who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

- The Headteachers and Senior Leaders together with all staff should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

The E-Safety Lead:

- Takes day-to day-responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policy/documents.
- Works with the Designated Child Protection Lead to address any Safeguarding issues. As detailed in our Child Protection and Safeguarding Policy.
- Is responsible for Smoothwall monitoring and filtering management in line with our Child Protection and Safeguarding Policy. Smoothwall notifications are logged and shared with governors termly.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- Provides training and advice for staff.
- Liaises with school ICT technical staff.
- Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments.

Teaching and Learning

The Internet is an essential element for education, business and social interaction. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils, and so the school has a duty to provide pupils with quality Internet access as part of their learning experience:

- The school Internet access will be designed expressly for pupil use including appropriate content filtering.
- Pupils will be given clear objectives for Internet use and taught what use is acceptable and what is not.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- As part of the new ICT (computing) curriculum, all year groups have digital literacy units that focus on different elements of staying safe online. These units include topics from how to use a search engine, digital footprints and cyber bullying.
- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.

Through ICT we ensure that the school meets the needs of all, taking account of gender, ethnicity, culture, religion, language, age, ability, disability and social circumstances. It is important that in this school we meet the diverse needs of pupils to ensure inclusion for all and that all pupils are prepared for full participation in a multi-ethnic society. We also measure and assess the impact regularly through meetings between our SENDCo and individual teachers to ensure all children have equal access to succeeding in this subject.

Pupils are taught in all lessons to be critically aware of the materials/content they access on-line and are guided to validate the accuracy of information

Target Tracker Link – Foundation Stage

With parental consent in Ash class, staff may share Learning Journeys with parents through the Target Tracker link. Please note, with the 2020 EYFS framework, the focus is on interacting with pupils, rather than recording observations. However, if observations are made, these may have images of other children who were part of the activity. Images must not be shared by parents outside the Target Tracker App.

Through the Target Tracker Link the Assessment Co-ordinator/EYFS staff can:

- Manage which home users are able to access observations

- Use the built-in review process to quality check observations, editing title and notes before making them available to home users
- Notify home users when new observations are added

Authorised Internet Access

By explicitly authorising use of the school's Internet access, pupils, staff, governors and parents are provided with information relating to e-safety and agree to its use:

- All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource.
- Parents will be informed that pupils will be provided with supervised Internet access and asked to sign and return a consent form for pupil access.
- Only authorised equipment, software and Internet access can be used within the school.

World Wide Web

The Internet opens up new opportunities and is becoming an essential part of the everyday world for children: learning, homework, sharing are some of the legitimate and beneficial uses. However, there are inappropriate and undesirable elements that must be managed:

- If staff or pupils discover unsuitable sites, the URL (address), time and content shall be reported to the teacher who will then complete an E-Safety Incident form and hand this immediately to the E-Safety Lead. The E-Safety Lead will report to the Headteacher, file the E-Safety Incident form in the HT files and complete the SLT E-Safety Log. The E-Safety Log will be reviewed termly by the E-Safety Lead.
- Pupils will be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.
- The school will work in partnership with the Local Authority to ensure filtering and monitoring systems are as effective as possible.

E-mail

- E-mail is a quick and easy method of communication, ensuring beneficial and appropriate usage is an important part of E-Safety:
- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Whole class or group e-mail addresses should be used in school rather than individual addresses.
- Access in school to external personal e-mail accounts is not allowed.
- E-mail sent to external organisations should be written carefully and authorised by the teacher before sending.
- Chain letters, spam, advertising and all other emails from unknown sources will be deleted without opening or forwarding.

Security and passwords

Passwords should be changed regularly. The system will inform users when the password is to be changed. Pupils and staff should never share passwords and staff must never let pupils use a staff logon. Staff must always 'lock' the PC if they are going to leave it unattended (the picture mute or picture freeze option on a projector will allow an image to remain on the screen and also allow a PC to be 'locked').

Virtual Learning Platform

An important aim of virtual learning platforms is to teach pupils how to interact safely and respectfully online. In order to learn how to do this, pupils will practise these skills and develop them in a safe environment. Our bespoke virtual learning platform has been set up to prevent cyber-bullying. This is achieved through:

- Restricting contact so that pupils can only message internal contacts (other Petersfield Pupils)
- The teachers can monitor messages sent between pupils

- We have set up a reporting system for pupils to notify teachers if a particular message has upset them

Blogging via the Virtual Learning Platform

At Petersfield we aim to give our pupils a voice and an audience through blogging. These are in the form of class blogs but can also be in the form of project blogs or individual pupil blogs. Our blogs will run via our Virtual Learning Platform and will:

- Safely give our pupils a wider audience for their learning
- Encourage reluctant learners to participate and succeed
- Allow pupils to receive quality feedback safely from many different people
- Allow pupils to peer assess each other's learning
- Encourage parental engagement
- Promote pupils' learning

E-Safety

Blogging involves pupils working on a dedicated part of the school's Virtual Learning Platform whilst in school and also at home. To be able to post, pupils need to log into the Virtual Learning Platform. The blogs will be sent to the class teacher for approval before appearing on the Virtual Learning Platform or school website.

Petersfield School seeks permission annually for photographs and videos.

In addition, the following are to be strictly adhered to:

- There is to be no identification of students using first name and surname; first name only is to be used
- All posted data must conform to copyright law; images, videos and other resources that are not originated by the school are not allowed unless the owner's permission has been granted or there is a licence which allows for such use (i.e. "creative commons").

Notice and take down policy – should it come to the school's attention that there is a resource which has been inadvertently uploaded, and the school does not have copyright permission to use that resource, it will be removed.

Incidents - Any E-Safety incident is to be brought to the immediate attention of the E-Safety Lead and Head Teacher. They will take the appropriate action to deal with the incident and to fill out an incident log.

Blog Rules:

Using a blog safely is the most important thing about being a blogger. The following rules, if followed, will minimise any risks and will ensure that pupils will stay safe whilst blogging. The blog rules are explained clearly to each class during launch and are displayed in the classes. Teachers will remind **the children about e-safety and blogging rules when they are blogging.**

Don'ts:

1. Never give away any personal information about your location or identity.
2. Don't post pictures of yourself without specific permission from your teacher or parents.
3. Never give out your log in details to anyone.
4. Don't use text language in your posts

Dos:

1. If you see anything that shouldn't be on your screen, do tell your teacher or parents immediately.
2. Try to post about things that your audience would like to read.
3. Try to show off your best work/writing whilst blogging and use the tips people suggest to you to improve.
4. Always tag your posts with your first name and include key words specific to your post.
5. Post things that interest you.
6. If you receive a comment, it is polite to respond, say thank you and reply to a question if they have left one.
7. If your post doesn't appear straight away, your teacher might be busy, do be patient.
8. Comment on other people's posts too. Blogging is about commenting and posting!
9. Do visit other class blogs regularly to read and comment. This helps people come back to your blog.

The Role of the Blog Admin/Teacher:

The blog admin normally is the class teacher. This responsibility as gatekeeper is key to ensuring safety for the pupils using the blog. The following guidelines should be followed if a successful flowing blog is to be achieved:

1. Visit the blog regularly. It is better to visit short and often than catching up once a week. Your bloggers will appreciate comments and posts being approved quickly!
2. If you use a shared computer, log out at the end of each session.
3. Promote the links on the class blog to the parents and the wider community.
4. A blog can take a while to gather momentum and an audience. Be patient... the audience will come!
5. Mention the blog in assemblies and have it on display at parent evenings or school events, a blogging culture will soon be established!
6. Make sure each blog looks different in your school. This will help keep the interest high for the pupils from year to year.
7. Visit other blogs regularly and promote these to your class through links on your blog. What goes around comes around with blogging and strong loyal communities will form quickly.

Social Networking and Chat Facilities

- Social networking Internet sites (such as, MySpace, Facebook, Whatsapp) provide facilities to chat and exchange information online. This online world is very different from the real one with the temptation to say and do things beyond usual face-to-face contact.
- Use of social networking sites and newsgroups in the school, is not allowed and will be blocked/filtered.
- Pupils will be advised never to give out personal details of any kind that may identify themselves, other pupils, their school or location. This will also include not using personal photographs and videos.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.
- Pupils will be encouraged to only interact with known friends, family and staff over the Internet and deny access to others.
- Parents, pupils and staff will be advised of the dangers of discussing pupils, staff or the school on social networking sites. The governors will consider taking legal advice, where appropriate, to protect pupils and staff against cyber bullying and defamatory comments.

Online Gaming

It is essential that children are aware of the potential issues regarding internet safety within the online gaming environment and are given the skills and knowledge to help manage and reduce these risks, with the help of those around them. At Petersfield, we follow the Childnet SMART Rules:

SMART rules

Safe: Keep safe by being careful not to give out personal information when playing online. This includes your e-mail address, phone number and password, as well as images and videos of yourself, friends and family

Meeting: Meeting someone you have only known online can be dangerous. Remember that no matter how long you have spoken to someone for, or how nice they are, if you have never met this person before then they are still a stranger. If anyone asks to meet up then tell an adult immediately.

Accepting: Accepting gaming requests, direct messages or clicking on links from people you don't know can lead to problems – they may contain viruses, inappropriate content or nasty messages!

Reliable: People we speak to online might not always be who they say they are as it is very easy to give away false information online. Try to only speak to your friends and family.

Tell: Tell your parent, carer or a trusted adult if someone or something makes you feel uncomfortable or worried, or if you or someone you know is being bullied online.

For a useful introduction to online gaming for parents, please see our website or:

<https://www.childnet.com/resources/online-gaming-an-introduction-for-parents/>

Reporting

All breaches of the E-safety policy should be Logged on MyConcern. The details of the user, date and incident should be reported. The category E-Safety should be selected.

Incidents which raise a concern, including a child protection concern should be addressed in line with our Safeguarding and Child Protection Policy and should be reported the same day.

Allegations involving staff should be reported to the Head Teacher. If the allegation is one of abuse then it should be handled according to the DFE document titled 'Dealing with allegations of abuse against teachers and other staff'. If necessary the local authority's Local Authority Designated Officer (LADO) should be informed.

Evidence of incidents must be preserved and retained.

The curriculum will cover how pupils should report incidents (e.g. CEOP button, trusted adult, Childline)

Mobile Phones and Devices

Many new mobile phones and devices have access to the Internet and picture and video messaging. Whilst these are the more advanced features, they present opportunities for unrestricted access to the internet and sharing of images. There are risks of mobile bullying, or inappropriate contact.

- Pupils should not have mobile phones or smart watches in school. Further information is detailed in the Mobile Phone and other Smart Devices Policy.
- Staff should always use the school phone to contact parents except in an emergency with permission from the Headteacher. If a personal device is used, the caller's ID should be blocked.
- Staff including students and visitors should not access or use their mobile phones within the classroom whilst pupils are present. All staff, visitors and volunteers should ensure that their phones do not ring and are not used and stored safely away during the teaching day. Where exceptions are made for specific purposes, including medical need, visits and administrative tasks, this will be authorised by the Headteacher and will follow identified rules.
- Parents cannot use mobile phones on school trips to take pictures of the children.
- On trips staff mobiles are used for emergency only.

Where a mobile phone is used as a medical device to manage an insulin pump, this must be detailed in their Individual Health Care Plan (IHCP). The device must be PIN protected with only identified staff (and the pupil if age appropriate) having knowledge of this PIN. The device must only be used as detailed in the IHCP and the child's parent is responsible for ensuring that the camera and other features not relevant to the IHCP are disabled.

Digital/Video Cameras/Photographs/Audio

Pictures, videos and sound may not be directly connected to the Internet but images are easily transferred.

- Pupils will not use digital cameras, video or recording equipment at school unless specifically authorised by staff.
- Publishing of images, video and sound will follow the policy set out in this document under 'Publishing Content'.
- **Parents/carers:**
 - Microsoft Teams video links are to be accessed by parents/carers of children by invitation only. Emails invitations contain joining instructions which must be followed at all times. These live video streams MUST NOT be viewed by anyone else. They must not be viewed in a public environment. Video links MUST NOT be shared to anyone else. If you would like another close family member or relative (e.g. grandparent) to attend a live video event, YOU MUST obtain specific permission from the school (via an email and the school office) **in advance** and by joining THEY MUST agree to follow our school policies.

- Please be aware that TEAMS sessions may be recorded. Even if your camera and microphone are off, your name may be visible on the recording. Parents/Carers should notify school staff if they do not want this to be so and they can be renamed whilst recording is in progress.
- At school events, if permitted, the member of staff will inform parent(s)/guardian(s) and others present at school events that photographs/videos/audio may be taken on the basis
 - That they are for private retention and not for publication in any manner
 - Parents/carers sign the Home School Agreement, to confirm that parents/carers and all family and friends who attend events agree that all photographs and recordings made are for private and personal use only following consent.
 - Such images should focus on your own child and photographs should not be taken of other children without their parents' permission except incidentally e.g. as part of a group shot
 - Images are for personal use, and are not published on social media, such as "Facebook and WhatsApp".
 - Anybody attending does not film/record/take images where copyright prevents this
 - Anyone attending does not film/record/take images in any circumstances that may embarrass or upset pupils.
 - Images, film or audio recording should not be made at any time without the intention to record being declared to the school and without the expressed consent of the staff involved and Head Teachers. The school reserves the right to refuse or withdraw permission for film, audio or photographs from anyone who does not follow these guidelines.
- Staff should always use a school camera to capture images and should not use their personal devices.
- Photos taken by the school are subject to the Data Protection Act.

Published Content and the School Website

The school website is a valuable source of information for parents and potential parents.

- Contact details on the Website will be the school address, e-mail and telephone number.
- Staff and pupils' personal information will not be published.
- One of the Head teachers or a nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.
- Photographs and videos that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Pupils' full names will not be used in association with photographs.
- Consent from parents will be obtained annually before photographs of pupils are published on the school website.
- Named work will only be published with the permission of the pupil.
- Parents should not upload any images from within school onto social networking sites.
- The Governing body may ban the use of photographic equipment by any parent who does not follow the school policy.

Information System Security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- Security strategies will be discussed with the Local Authority.
- E-safety will be discussed with our ICT support and those arrangements incorporated in to our agreement with them.

Protecting Personal Data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and Freedom of Information Act.

Assessing Risk

The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school does not accept liability for the material accessed, or any consequences of Internet access. The school will audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.

Handling E-Safety Complaints

- Complaints of Internet misuse will be dealt with in line with our Positive Behaviour and Complaints Procedures.
- Any complaint about staff misuse must be referred to one of the Headteachers.
- Complaints of a child protection nature shall be dealt with in accordance with school child protection procedures.
- Pupils and parents can access the Complaints Policy on the school website.
- Discussions will be held with the community police officer to establish procedures for handling potentially illegal issues.

Communication of Policy

Pupils:

- Rules for Internet access will be posted in all networked rooms.
- Pupils will be informed that Internet use will be monitored.
- Pupils will be informed of the importance of being safe on social networking sites. This will be strongly reinforced across all year groups during Computing lessons and all year groups look at different areas of safety through the digital literacy lessons.

Staff:

- All staff will be given the School E-safety Policy and its importance explained.

Parents:

- Parents' attention will be drawn to the School e-safety Policy in newsletters and on the school Website.
- Parents, staff and Governors sign to agree to the ICT policy annually.

Further Resources

We have found these web sites useful for E-Safety advice and information.

http://www.thinkuknow.co.uk/	Set up by the Police with lots of information for parents and staff including a place to report abuse.
http://www.childnet-int.org/	Non-profit organisation working with others to "help make the Internet a great and safe place for children".

Appendix 1 – Acceptable Use for Data Processors (adult)

A: Use of school based equipment and services

Access to school equipment, the school network and the internet

- I will access the internet and other ICT systems using an individual username and password, which I will keep secure. I will ensure that I log out after each session and never allow other users to access the internet through my username and password. I will report any breach of security to the E-safety coordinator/Headteacher.
- I will not search for, download, upload or forward any content that is illegal or that could be considered an offence by another user. If I encounter any such material I will report it immediately to the e-safety coordinator/ Headteacher. I will not download or install any software from the internet or from any other media which may compromise the school network or information situated on it.
- I will not attempt to bypass any filtering and/or security systems put in place by the school. If I suspect a computer or system has been damaged or affected by a virus or other malware, I will report this to the e-safety coordinator.
- I will seek written consent from the E-safety coordinator/ headteacher prior to the use of any new technologies (hardware, software, cloud-based services) within school.
- I understand that my files, communications and internet activity may be monitored.

Creation, storage and security of digital content

- I will take reasonable precautions to ensure that any devices (laptops, tablets, cameras, removable media or phones) are stored in a secure manner when taken off site (car / home/ other location). Devices will not be stored in a car unattended or left in sight when not in use, e.g. by an open window. I will ensure that any personal or sensitive information taken off site will be situated on a school-owned device with appropriate technical controls such as encryption / password protection. If using my own device at home to view data, I will ensure that it is encrypted / password protected.
- I will use only school-provided portable storage (USB sticks, SD cards, portable hard drives etc) with encryption unless permission has been granted by the E-safety coordinator / Headteacher.
- I will demonstrate professional, safe and responsible behaviour when creating, using and storing digital images, video and sound within school. I will model safe and responsible behaviour in the creation and publishing of online content.
- I will use only school equipment to create digital images, video and sound unless prior permission is granted by the E-safety coordinator / Headteacher.
- I will ensure that I am familiar with the current permission status of pupils (see Parental Consent Form for Digital Images and Video). A summary of all permissions are circulated to all staff and available from the office. If additional permission is needed, e.g. for a surname in the press or for a medical form on SIMS, then I will discuss this with the E-safety coordinator and further written permission will be sought.
- I will ensure that I am familiar with the current Data Protection Policy. I will manage my digital files in accordance with this and I will make myself familiar with procedures in case of a breach of data security.
- I will not leave my computer unattended whilst working on screen; instead I will press CTL/ALT/HLT to lock the screen.
- I will only store / retain data files in line with the Data Retention Policy and will be responsible for deleting files which are no longer required.

School email and calendars

- I will use my school email address for all school-related correspondence. I understand that any use of the school email system will be monitored and checked. I will not use my private email account for any school-related business. Email is the main method of communication for all school matters and I will check my e-mail regularly and respond in a timely manner (in normal working hours) to communications that require my attention.
- I will take care in opening any attachments sent by email. I will only open emails and associated attachments from trusted senders.

- Communication between staff or members of the wider school community should be professional and related to school matters only. Emails sent to external organisations will be written carefully and if necessary authorised before sending to protect members of staff. All communications to parents and carers should be sent to the office email account for onward transmission. It is best practice when emailing parents and/or carers to add all intended recipients to the BCC address field. This ensures that parents' personal email addresses are not visible to others.
- To avoid the misrepresentation of others I will not make changes to someone else's e-mail and then pass it on without making it clear where changes have been made.
- I will take great care when forwarding messages to ensure that no confidential or sensitive material (e.g. other's email addresses) are attached
- The school calendar on Central Hosting is the central calendar for all school matters. I will check it regularly and take events into account when planning lessons and visits etc. I will add events and appointments to the diary dates as necessary. I will also regularly check the school website calendar.

Learning and teaching

- In line with every child's legal entitlement I will ensure I teach / model an age-appropriate e-safety curriculum.
- I will support and promote the school e-safety policy at all times. I will model safe and responsible behaviour to pupils when using ICT to support learning and teaching.
- I will ensure that I am aware of my individual responsibilities relating to the safeguarding of children within the context of e-safety and know what to do in the event of misuse of technology by any member of the school community.
- I understand the importance of respecting and acknowledging copyright of materials found on the internet and will model best practice in the creation of my own resources at all times.
- I will ensure that all online services and software that I use as part of my teaching are appropriate and are used in line with current guidance.
- I agree to adhere by the school's Prevent guidelines and action plan.

B: Personal equipment and services

Social media and messaging

- I will not talk about my professional role in any capacity when using personal social media. I will not use social media tools to communicate with current or former pupils under the age of 18 nor to communicate with parents in a professional capacity. I will be mindful of potential conflicts of interest where a parent or carer of a child at the school is also a personal friend. I will set and maintain my profile on social networking sites to maximum privacy. I will not access social networking sites for personal use during school hours.
- If I experience any derogatory, negative or slanderous comments relating to the school, colleagues or my professional status, I will take screenshots for evidence and bring this to the attention of the e-safety coordinator or Headteacher.
- Use of school equipment or e-mail accounts for personal financial gain, gambling, political purposes or advertising is forbidden. However, nothing in this paragraph is intended to restrict members of staff conducting any trade union or professional association using school computers or e-mail accounts, outside of teaching hours.

Personal mobile phones and other devices

- I will not bring my mobile into teaching spaces unless with the overt permission of the Headteacher. If permitted, I will ensure that my mobile phone and any other personally-owned device is switched off or switched to silent mode and out of sight during teaching hours and used only in emergencies.
- I will not contact any parents or pupils on my personally-owned device unless in an emergency. If a pupil or parent contacts me using my personal device I will inform the Headteacher as soon as possible. On educational visits my personal mobile phone may be used to contact the school.
- I will not use any personally-owned mobile device to take images, video or sound recordings in school without the overt, written permission of the Headteacher.

- I will seek permission from the E-safety coordinator / Headteacher if I need to synchronise any school email account with a personally-owned device. If permission is granted then I will ensure that the device has the appropriate technical controls such as encryption / password protection.

Data Processors found to be in breach of these rules may face disciplinary action in line with the school's disciplinary procedures.

Full name (Please print): _____

Signed: _____

Date: _____

Addendum to pupil Acceptable Usage Policy (AUP)

Remote Learning and using Microsoft Teams

As we are all now using the internet more, including home learning (HL) platforms, the following has been added as an addendum to the existing Petersfield School AUP (see below).

- **Parents/carers:** Microsoft Teams video links are to be accessed by parents/carers of children by invitation only. Emails invitations contain joining instructions which must be followed at all times. These live video streams **MUST NOT** be viewed by anyone else. They must not be viewed in a public environment. Video links **MUST NOT** be shared to anyone else. If you would like another close family member or relative (e.g. grandparent) to attend a live video event, **YOU MUST** obtain specific permission from the school (via an email and the school office) **in advance** and by joining **THEY MUST** agree to follow our school policies.
- **Please be aware that sessions may be recorded.** Even if your camera and microphone are off, your name may be visible on the recording. Parents/Carers should notify school staff if they do not want this to be so and they can be renamed whilst recording is in progress. Please ensure that your use of IT, both in school and outside of school, on personal and school owned devices, will not cause Petersfield School, staff, pupils or others distress or bring your or their character into disrepute.

Please note that Microsoft Teams is not to be used as a communication platform but as a tool to set and receive work remotely and for teachers to connect with children virtually in the case of a further lockdown. All electronic communications should be directed to the class teacher through the office@petersfield.cambs.sch.uk email address.

- When using Microsoft Teams 'chat' remember that everyone in your class could see what you post including your teacher. It is therefore very important that you think carefully before you post anything. Inappropriate comments will be dealt with and your parents may be informed.
- Any recordings must not, under any circumstances, be saved, forwarded or posted on any other online platform, including social media, without the permission of that member of staff.
- Pupils are unable/may not attempt to call, chat or set up private groups between each other on Microsoft Teams (this feature has been disabled).
- Pupils are unable/may not attempt to start or record a meeting/lesson (this feature has been disabled).
- Pupils are not permitted to share recorded videos/lessons/narrated PowerPoint Presentations made by teachers within or outside of the Petersfield Teams Account.
- Pupils should blur their background if in a conference meeting which involves a camera (if this facility is available to them).
- Pupils should think carefully about what is acceptable language with regards to what they type and post.
- Pupils must hang up at the end of the lesson once instructed to do so. The teacher must be the last person in the meeting to hang up.
- You must only ever use school channels to communicate with a member of staff. These channels are your class email address and Microsoft Teams. Members of staff will use their class email address and Microsoft Teams to communicate with you.

Your safety is of paramount importance. You may be spending more time online and this puts you at a higher risk of negative experiences. Other people on line may not be who they say they are or may be looking to exploit young people. They are using this time of extra use to initiate more contact. People are anxious and struggling with the changes happening and feelings of isolation and they may take this out on other people online by being unkind and bullying.

It is essential therefore, that you are aware of the following ways to report or raise concerns whilst online:

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

You can also report concerns to your parents and members of staff at school, via email or Microsoft Teams. Just because you are not seeing staff every day, does not mean they are not still here for you if you need them. If something is worrying you, whether it is something to do with being online or not, reach out. We will do everything we can to support you.

Microsoft Teams sessions protocol for parents/carers:

Important disclaimer: By accessing the MS Team meeting, you are agreeing to share your personal information and data within a controlled school group. You are also agreeing to the terms of use below.

Please be aware that the following apply to live sessions:

- A grown up must oversee their child/ren on the Team meeting
- Switch the settings to have microphones off and videos off when joining a session.
- Sessions are **NOT** to be recorded by parents or pupils.
- During sessions, screen shots using the device or other devices are strictly **NOT** allowed.
- Learn how to mute and unmute, including video screens.
- Be conscious of background environments and others in the room.
- Pupils must wear suitable clothing, as should anyone else in the household.
- Any computers used should be in appropriate areas, for example, not in bedrooms; and where possible be against a neutral background.
- Language must be professional and appropriate, including any family members in the background.
- Videos may be muted for pupils if other children in the household become unsettled or cause a disruption.
- Please note if you are late for the session, you can still join.

Petersfield School reserves the right to record all sessions for safeguarding and teaching reasons. These recordings will be stored safely on the school server and removed in compliance with our GDPR policy for data retention.

Helpful tips for children's success using MS Teams:

- Make sure you are muted when not talking.
- Be yourself and respect others – think about what you are going to say.
- Ask questions using chat function (when enabled) or put your hand up using the hand feature if wanting to ask a question live.
- Use reactions to engage with your class.
- Think before you write.
- If any behaviour is deemed not appropriate, pupils will be warned once then the next time removed from the chatroom.
- Focus on what is being taught or said, rather than distracting others.
- Make sure the adult you see is a known member of staff.

Think before you click

S



I will only use the Internet and email with an adult's permission.

A



I will only click on icons and links when I know they are safe.

F



I will only send friendly and polite messages.

E



If I see something I don't like on a screen, I will always tell an adult.

Child's name: _____

Child's signature: _____

I will support the school by promoting safe use of the Internet and digital technology at home and will inform the school if I have any concerns over my child's e-safety. I will support the school's approach to e-Safety and will not upload or add any pictures, audio, video or text onto any social media that could comment on, upset, offend, identify or threaten the safety of any member of the school community. I have read and agree to the E-safety and Data Protection policies, including the Addendum to pupil Acceptable Usage Policy (AUP) – 1st September 2024, and agree to follow this.

Parent's signature: _____ Date: _____

Appendix 3 – KS2 Acceptable Usage Policy

Petersfield Church of England Aided Primary School **Pupil KS2 Rules for Responsible Internet Use**

These rules will keep me safe and help me to be fair to others:

- I will ask permission to go online.
- I will only edit or delete my own files and not look at, or change, other people's files without their permission.
- I will not bring files into school without permission or upload inappropriate material to my workspace.
- I am aware that some websites and social networks have age restrictions and I should respect this.
- I will not attempt to visit Internet sites that I know to be banned by the school.
- I will only e-mail people I know, or a responsible adult has approved.
- The messages I send, or information I upload, will always be polite and sensible.
- I will not open an attachment, or download a file, unless I know and trust the person who has sent it.
- I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless a trusted adult has given permission. I will never arrange to meet someone I have only ever previously met on the Internet, unless my parent/carer has given me permission and I take a responsible adult with me.
- If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will show a teacher / responsible adult.
- If I need to bring a phone to school, I will pass it to the office for safe keeping.
- If I use material that is the work of others in my work, I will state where I found the information.
- I will use a range of passwords, keep all passwords safe and never share accounts.

I have read and understand these rules and agree to them.

Child's name: _____ Child's signature: _____

I will support the school by promoting safe use of the Internet and digital technology at home and will inform the school if I have any concerns over my child's e-safety. I will support the school's approach to e-Safety and will not upload or add any pictures, audio, video or text onto any social media that could comment on, upset, offend, identify or threaten the safety of any member of the school community. I have read and agree to the E-safety and Data Protection policies, including the Addendum to pupil Acceptable Usage Policy (AUP) – 1st September 2024, and agree to follow this.

Parent's signature: _____ Date: _____

The school accepts no responsibility for inappropriate use of the Internet outside school, even when children are researching a school-based subject.

Appendix 3 - Guidance for safer working practice for those working with children and young people in education settings

Staff engaging in online learning should display the same standards of dress and conduct that they would in the real world; they should also role model this to pupils and parents.

Staff Expectations

Staff Should:

- think about the background; photos, artwork, identifying features, mirrors – ideally the backing should be blurred
- staff should be in living / communal areas – no bedrooms
- staff should be fully dressed
- adhere to Petersfield School's E-Safety Policy
- ensure that a senior member of staff is aware that the online lesson / meeting is taking place and for what purpose
- avoid one to one situations – request that a parent is present in the room for the duration, or ask a colleague or member of SLT to join the session or be present in person
- only record a lesson or online meeting with a pupil where this has been agreed with the head teacher or other senior staff, and the pupil and their parent/carer have given explicit written consent to do so
- ensure resources / videos must be age appropriate – the child may not have support immediately to hand at home if they feel distressed or anxious about content

Staff should not:

- contact pupils outside the operating times defined by senior leaders
- take or record images of pupils for their personal use
- record virtual lessons or meetings using personal equipment (unless agreed and risk assessed by senior staff)
- engage online while children are in a state of undress or semi-undress

It is the responsibility of the staff member to act as a moderator; raise any issues of suitability (of dress, setting, behaviour) with the child and / or parent immediately and end the online interaction if necessary. Recording lessons does not prevent abuse. If staff wish to record the lesson they are teaching, consideration should be given to data protection issues; e.g., whether parental / pupil consent is needed and retention / storage. If a staff member believes that a child or parent is recording the interaction, the lesson should be brought to an end or that child should be logged out immediately. Staff, parent and pupil Acceptable Usage Policy (AUP) should clearly state the standards of conduct required.

Appendix 4: Keeping students safe while using meetings in Microsoft Teams for distance learning: Guidance For Petersfield Staff

Learning online can be just as personal, engaging, and socially connected as learning in a classroom. Educators and teachers can stay in touch and help each other using Teams chats and can feel like they're meeting in person using live meetings.

However, online learning also requires educators and administrators to set up certain policies and restrictions to guard students' safety. These policies can prevent unauthorized users from gaining access to online meetings, can allow educators to quickly and easily remove inappropriate messages, and manage student disruptions.

For administrators

Set up identities for your students and educators

We strongly recommend that you create student identities for distance learning. Requiring students and educators to sign in to Teams before they join meetings is the safest meeting setup for remote learning during lessons.

If accessing Teams when not signed in, safety measures will be enabled, e.g. controlling who can enter the meeting/let people into the meeting, controlling who can comment/speak/use emoji's, using the facility to eject people from a meeting if necessary and controlling who can present during the meeting.

For more information on how you can setup identities and licenses for your organization, visit our [Get started with Microsoft Teams for remote learning](#) guide.

Set policies for students, educators, and organizations

[Teams policies](#) allow you to control many of the options available for your organization and for specific users. They include the ability to control who can use private chat and private calling, who can schedule meetings, and what content types can be shared.

Policy settings for your organization

There are many different policy settings you can configure in your organization. One of the most important policies you can set to enhance students' safety is to restrict the ability of anonymous users to join meetings. This requires all meeting attendees to be signed in with an account from your organisation.

If you have provided your students and educators with Teams licenses and do not plan to allow participants to join meetings without signing in to Teams, ensure that the following policy is set:

- **Anonymous users can join a meeting:** *Off*

Policy settings for students

We recommend you create student identities in your tenant for distance learning. To create a path with the greatest safety, we strongly recommend requiring students to sign in to Teams in order to join meetings.

Limit students' ability to schedule meetings and private calls

You can use the following Teams policies to limit a student's ability to both schedule meetings and initiate private calls with faculty and other students.

- [Meeting policies](#)
- **Allow Meet now in channels:** *Off*
- **Allow the Outlook add-in:** *Off*
- **Allow channel meeting scheduling:** *Off*
- **Allow scheduling private meetings:** *Off*
- **Allow Meet now in private meetings:** *Off*
- [Live events policies](#)
- **Allow scheduling:** *Off*
- [Calling policies](#)

- **Make private calls:** *Off*
Policy settings for educators

You can use additional policy settings to help educators control access to their meetings, monitor chat sessions, and remove inappropriate messages.

Allow educators to control access to their meetings

The following settings help your educators have the strictest control over who has access to their online meetings.

- Meeting policies
- **Let anonymous people start a meeting:** *Off*
- **Automatically admit people:** *Everyone in your organization*
- **Allow dial-in users to bypass the lobby:** *Off*

Allow educators to monitor chat sessions and remove inappropriate messages in channel meetings

- Messaging policies
- **Owners can delete sent messages:** *On*

Note: This allows educators to remove inappropriate messages in class chats when the meeting is created within the channel, or to remove messages within the channel itself.

For educators

Switching to distance learning can present a new set of challenges for your teaching. Microsoft Teams can help you create and run online meetings for your class and provide a safer, controlled learning environment for your students.

Typical tasks include: scheduling meetings, showing video, sharing PowerPoint presentations, and recording a meeting.

You can also invite external speakers for virtual field trips.

Scheduling your meetings

When you schedule a meeting in Teams for online lectures or guest speaker sessions, we recommend you create those meetings in channels. Channels give you more robust controls within meetings such as disabling student-to-student chat, providing an easier meeting setup process, and giving you the ability to track class discussions in context.

We have two video tutorials that will help you use Microsoft Teams to schedule your online meetings and maximize student safety. Check out Online Lectures 101 - keeping your online lectures as safe as possible and Online classes and lectures with your students - scheduling meetings.

Settings to change before a meeting

As the meeting organizer, you should manage several options to increase your students' online safety. To see and change these settings, you can go to Meeting Options using the link included in the meeting invitation information provided when you created the meeting.

- Change **Who can bypass the lobby** to *People in my organization*
- This setting ensures that anyone who isn't signed in with an account from your educational institute will need to wait in the meeting lobby until you join the meeting and admit them.
- Change **Always let callers bypass the lobby** to *No*
- This setting ensures that anyone joining the meeting over the phone rather than using Teams will need to wait in the meeting lobby until you join the meeting and admit them.
- Change **Who can present** to *Only me*
- Setting this option ensures that other participants will join the meeting as attendees. The attendee role doesn't allow them to mute other participants, remove participants, or admit anyone from the lobby. Attendees can still share video, participate in the meeting chat, and view shared files in the meeting. You can learn more about meeting roles in Roles in a Teams meeting.

If your students join the meeting before you, you'll receive a notification in Teams. You can then ask the students to leave the meeting until the lecture starts.

As the meeting organizer, you can also select **Show participants** in the meeting controls and remove students manually, or end the meeting completely using the **end meeting** feature.

At the start of a meeting

Here are a few tips to help you curate a controlled and safer environment for your students when using Teams meetings.

1. Review and admit invited guests who are waiting in the lobby.
2. Double check the list of participants in your meeting to make sure your students are all present and that there aren't any unexpected attendees. You can do this by selecting **Show participants** in the meeting controls.
3. Turn on background blur for your video and ask your students to do so as well.
4. Ask students to pin your video. They can use the **More ...** menu next to your name to do this. Let students know that you're muting their audio, then from the participants list, click **Mute all**. If you plan on recording the video for the meeting, make sure the students' videos are turned off or, that you have consent to record the students' videos. In the case of primary and secondary students, you should ensure that you have a parent or guardian's consent before recording.

During the meeting

Here are a few tips you can use during a meeting to maximize students' safety.

1. If others need to present content during the meeting, whether the content is from other students or colleagues, you can promote an attendee to presenter during the meeting. Hover over the person's name, then select **More options > Make a presenter**. When the person is done presenting, hover over their name again and select **More options > Make an attendee**.
2. Check that all students are muted unless they're asking a question.
3. Keep an eye on the meeting chat to check for questions. If you see inappropriate messages, you can either delete them or mute the student for a time. This feature is only available if you create the meeting as a channel meeting. For more information, see Mute student comments in a class team and Edit or delete a sent message in Teams.
4. Warn misbehaving students or remove them from the meeting by using **Show participants** in the meeting controls.

After the meeting

At the end of the meeting, click the three dots in meeting controls and select **End Meeting**. This will end the meeting for all participants.

Once the meeting ends, any student attempting to join the meeting will send a Teams notification to the meeting organizer. You can then ask the student or students to leave the meeting since it has already ended.

If they don't leave, you can remove them from the meeting by using **Show participants** in the meeting controls.

If you're away from your notifications for a time, you can also monitor the meeting's chat window to see if any students have re-joined the meeting after it ends.

Staff Safeguarding Protocols for meetings or live streams with children

1. Parents will be informed that teachers may schedule live sessions. These will be scheduled using an invitation through Teams. Online video lessons will only take place during the school day.
2. If recording videos or livestreaming lessons, make sure to film in a neutral area where nothing personal or inappropriate can be seen or heard in the background. Ensure you are dressed appropriately for the meeting.

3. Where possible, use the opportunity to share your screen rather than a video of yourself. Ensure you are not sharing any personal data (close tab and files that are not relevant to your meeting, close your emails to prevent email previews appearing in shot).
4. Please only use Teams for live streaming or video conferencing with children. Do not accept students into a video conference if they are using their personal credentials. They must sign in using their school account. **Staff should never contact students using their personal accounts.**
5. Only the teacher should be hosting a session. Do not join sessions that are hosted by students.

Groups of Students (for example: live lessons)

6. Ask students to switch their video cameras off and keep their voice muted, unless they need to speak.
7. Do not start the lesson until you have more than two students present in the meet. Keep your camera off and microphone muted until you are ready. Always try to record any live sessions that you run from the moment you begin to interact with the students.
8. If you would usually have a Teaching Assistant or another adult in the class, don't forget to invite them and encourage them to participate as well.

Sessions for Individual students (For example, pastoral sessions)

9. If you have arranged an individual session, for example a pastoral session, please ensure parents / carers are around for the meeting. This needs to be arranged in advance of the meeting.
10. If students are required to show video, ensure the students are within a communal space in their home (not a bedroom), they are dressed appropriately (not in their PJs) and parents or carers are present.
11. Ensure your line manager is aware these online sessions are taking place and when they are scheduled.

Safeguarding Concerns

12. If you have a safeguarding concern, be sure to log this in the normal way using MyConcern form. If you feel the child is at immediate risk of harm, please contact a safeguarding lead as soon as possible.

Behaviour and Conduct: Things to consider

- Live streaming lessons to children is not a default continuous expectation. There are other ways to ensure children are engaging with their learning, including setting tasks on Teams/Show My Homework or using quizzes or other online software.
- Assess the risks before you start the live lesson. Children are able to communicate with each other, without you knowing, record video, take screenshots and distribute images or videos that have been adapted.
- Keep it simple. Think about the timing, duration, participants and task.
- Consider students who will not be able to access these lessons. How will you support these students so they don't miss the same learning opportunity? Consider publishing resources used as part of the lesson.