# The Pears Family Charitable Foundation School

# ICT & Internet Acceptable Use Policy

| | |
|---|---|
| Date most recently Approved by Governors | Sept 2026 |
| Review Date | Sept 2027 |
| Coordinator | Head of Care, MH & Safeguarding Lead |
| Head Techer Signature | |

**At the heart of all policies at The Pears Family School are the following principles:**

- Every young person in our school, whatever their personal circumstances can learn and achieve.
- Every young person in our school, whatever their self-perception and previous experiences, has academic and creative potential to become a valuable member of society.
- The key to learning at The Pears Family School lies within the quality of the relationships between pupils, family members, staff and the intermediate agencies with whom we work.
- The success of our school is based on high expectations, mutual trust, caring for each other and taking responsibility.
- Every young person in our school is capable of becoming an agent for change in his or her local community.
- Under the Equality Act 2010 we have a duty not to discriminate against people on the basis of their age, disability, gender, gender identity, pregnancy or maternity, race, religion or belief and sexual orientation
- We have carefully considered the impact of this policy on equality and the possible implications for pupils with protected characteristics, as part of our commitment to meet the Public Sector Equality Duty (PSED) requirement to have due regard to the need to eliminate discrimination, advance equality of opportunity and foster good relations

# The Pears Family Charitable Foundation School

## Contents


1. Introduction and aims ..... 2
2. Relevant legislation and guidance ..... 2
3. Definitions ..... 3
4. Unacceptable use ..... 3
5. Staff (including governors, volunteers, and contractors) ..... 4
6. Pupils ..... 6
7. Parents ..... 7
8. Data security ..... 7
9. Internet access ..... 8
10. Monitoring and review ..... 9
11. Related policies ..... 9
    Appendix 1: Facebook cheat sheet for staff ..... 10
    Appendix 2: Acceptable use of the internet: agreement for parents and carers ..... 12
    Appendix 3: Acceptable use agreement for older pupils ..... 13
    Appendix 4: Acceptable use agreement for younger pupils ..... 14
    Appendix 5: Acceptable use agreement for staff, governors, volunteers and visitors ..... 15
    Appendix 6: Online safety contract Pupils and Families


## 1. Introduction and aims

ICT is an integral part of the way our school works, and is a critical resource for pupils, staff, governors, volunteers and visitors. It supports teaching and learning, pastoral and administrative functions of the school.

However, the ICT resources and facilities our school uses also pose risks to data protection, online safety and safeguarding.

This policy aims to:

- Set guidelines and rules on the use of school ICT resources for staff, pupils, parents and governors
- Establish clear expectations for the way all members of the school community engage with each other online
- Support the school's policy on data protection, online safety and safeguarding
- Prevent disruption to the school through the misuse, or attempted misuse, of ICT systems
- Support the school in teaching pupils safe and effective internet and ICT use

This policy covers all users of our school's ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors.

Breaches of this policy may be dealt with under our staff code of conduct.

## 2. Relevant legislation and guidance

This policy refers to, and complies with, the following legislation and guidance:

- Data Protection Act
- The General Data Protection Regulation
- Computer Misuse Act 1990
- Human Rights Act 1998
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Education Act 2011
- Freedom of Information Act 2000
- Searching, screening and confiscation: advice for schools
- Keeping Children Safe in Education 2026
- Children's Wellbeing & Schools Act 2026 – Section 36 - https://www.gov.uk/government/publications/mobile-phones-in-schools/mobile-phones-in-schools

## 3. Definitions

- **"ICT facilities":** includes all facilities, systems and services including but not limited to network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, and any device system or service which may become available in the future which is provided as part of the ICT service.
- **"Users":** anyone authorised by the school to use the ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors.
- **"Personal use":** any use or activity not directly related to the users' employment, study or purpose.
- **"Authorised personnel":** employees authorised by the school to perform systems administration and/or monitoring of the ICT facilities.
- **"Materials":** files and data created using the ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites, and blogs.

## 4. Unacceptable use

The following is considered unacceptable use of the school's ICT facilities by any member of the school community. Any breach of this policy may result in disciplinary or behaviour proceedings (see section 4.2 below).

Unacceptable use of the school's ICT facilities includes:

- Using the school's ICT facilities to breach intellectual property rights or copyright.
- Using the school's ICT facilities to bully or harass someone else, or to promote unlawful discrimination.
- Breaching the school's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity.
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate.
- Activity which defames or disparages the school, or risks bringing the school into disrepute.
- Sharing confidential information about the school, its pupils, or other members of the school community
- Connecting any device to the school's ICT network without approval from authorised personnel

- Setting up any software, applications or web services on the school's network without approval by authorised personnel, or creating or using any program, tool or item of software designed to interfere with the functioning of the ICT facilities, accounts or data.
- Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel.
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities.
- Causing intentional damage to ICT facilities
- Removing, deleting or disposing of ICT equipment, systems, programs or information without permission by authorised personnel
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation.
- Promoting a private business, unless that business is directly related to the school.

Using websites or mechanisms to bypass the school's filtering mechanisms.

This is not an exhaustive list. The school reserves the right to amend this list at any time. The Head Teacher will use professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the school's ICT facilities.

### 4.1 Exceptions from unacceptable use

Where the use of school ICT facilities is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the Head Teacher's discretion.

Permission must be sought in writing to the Head Teacher for approval.

### 4.2 Sanctions

Pupils and staff who engage in any of the unacceptable activity listed above may face disciplinary action in line with the school's policies on staff code of conduct. A copy of the staff code of conduct can be found on the school website.

## 5. Staff (including governors, volunteers, and contractors)

### 5.1 Access to school ICT facilities and materials

The school's business manager and Head Teacher manages access to the school's ICT facilities and materials for school staff. That includes, but is not limited to:

- Computers, tablets and other devices
- Access permissions for certain programmes or files

Staff will be provided with unique log-in/account information and passwords that they must use when accessing the school's ICT facilities.

Staff who have access to files they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the school business manager or Head Teacher.

#### 5.1.1 Use of phones and email

The school provides each member of staff with an email address.

This email account should be used for work purposes only.

All work-related business should be conducted using the email address the school has provided.

Staff must not share their personal email addresses with parents and pupils.

Staff must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.

Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents. Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.

Staff must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient.

If staff receive an email in error, the sender should be informed and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.

If staff send an email in error which contains the personal information of another person, they must inform the Head Teacher immediately and follow our data breach procedure.

Staff should use phones provided by the school to conduct all work-related business.

School phones must not be used for personal matters.

Staff who are provided with mobile phones as equipment for their role must abide by the same rules for ICT acceptable use as set out in section 4.

## 5.2 Personal use

Staff are permitted to occasionally use school ICT facilities for personal use subject to certain conditions set out below. Personal use of ICT facilities must not be overused or abused. The business manager and Head Teacher may withdraw permission for it at any time or restrict access at their discretion.

Personal use is permitted provided that such use:

- Does not take place during contact time with pupils
- Does not constitute 'unacceptable use', as defined in section 4
- Takes place when no pupils are present
- Does not interfere with their jobs, or prevent other staff or pupils from using the facilities for work or educational purposes

Staff should be aware that use of the school's ICT facilities for personal use may put personal communications within the scope of the school's ICT monitoring activities (see section 5.5). Where breaches of this policy are found, disciplinary action may be taken.

Staff should be aware that personal use of ICT (even when not using school ICT facilities) can impact on their employment by, for instance putting personal details in the public domain, where pupils and parents could see them.

Staff should take care to follow the school's guidelines on social media (see appendix 1) and use of email (see section 5.1.1) to protect themselves online and avoid compromising their professional integrity.

### 5.2.1 Personal social media accounts

Members of staff should ensure that their use of social media, either for work or personal purposes, is appropriate at all times.

The school has guidelines for staff on appropriate security settings for Facebook (and all other social media) accounts (see appendix 1).

### 5.3 Remote access

We allow staff to access the school's ICT facilities and materials remotely.

Staff accessing the school's ICT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on-site. Staff must be particularly vigilant if they use the school's ICT facilities outside the school and take such precautions as the Business Manager/Head Teacher may require from time to time against importing viruses or compromising system security.

Our ICT facilities contain information which is confidential and/or subject to data protection legislation. Such information must be treated with extreme care and in accordance with our data protection policy, which can be found on the school website.

### 5.4 Monitoring of school network and use of ICT facilities

The school reserves the right to monitor the use of its ICT facilities and network. This includes, but is not limited to, monitoring of:

- Internet sites visited
- Bandwidth usage
- Email accounts
- Telephone calls
- User activity/access logs
- Any other electronic communications

Only authorised ICT staff may inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law.

The school monitors ICT use in order to:

- Obtain information related to school business
- Investigate compliance with school policies, procedures and standards
- Ensure effective school and ICT operation
- Conduct training or quality control exercises
- Prevent or detect crime
- Comply with a subject access request, Freedom of Information Act request, or any other legal obligation

## 6. Pupils

### 6.1 Access to ICT facilities

- "Computers and equipment at school are available to pupils only under the supervision of staff"
- "Specialist ICT equipment, such as that used for music or design and technology must only be used under the supervision of staff"

### 6.2 Search and deletion

Under the Education Act 2011, and in line with the Department for Education's guidance on searching, screening and confiscation, the school has the right to search pupils' phones, computers or other devices for pornographic images or any other data or items banned under school rules or legislation.

The school can, and will, delete files and data found on searched devices if we believe the data or file has been, or could be, used to disrupt teaching or break the school's rules.

### 6.3 Unacceptable use of ICT and the internet outside of school

The school will sanction pupils, in line with the behaviour for learning policy, if a pupil engages in any of the following **at any time** (even if they are not on school premises):

- Using ICT or the internet to breach intellectual property rights or copyright
- Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, other pupils, or other members of the school community
- Gaining or attempting to gain access to restricted areas of the network, or to any password protected information, without approval from authorised personnel
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities
- Causing intentional damage to ICT facilities or materials
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation
- Using inappropriate or offensive language

## 7. Parents

### 7.1 Access to ICT facilities and materials

Parents do not have access to the school's ICT facilities as a matter of course.

Parents working with the school as part of the Family Model upon which we operate may be granted an appropriate level of access or be permitted to use the school's facilities at the school's discretion.

### 7.2 Communicating with or about the school online

We believe it is important to model for pupils, and help them learn, how to communicate respectfully with, and about, others online.

Parents play a vital role in helping model this behaviour for their children, especially when communicating with the school through our website and social media channels.

We ask parents to sign the agreement in appendix 2.

## 8. Data security

The school takes steps to protect the security of its computing resources, data and user accounts. However, the school cannot guarantee security. Staff, pupils, parents and others who use the school's ICT facilities should use safe computing practices at all times.

### 8.1 Passwords

All users of the school's ICT facilities should set strong passwords for their accounts and keep these passwords secure and updated on a regular basis.

Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control.

Members of staff or pupils who disclose account or password information may face disciplinary action. Parents or volunteers who disclose account or password information may have their access rights revoked.

### 8.2 Software updates, firewalls, and anti-virus software

All of the school's ICT devices that support software updates, security updates, and anti-virus products will be configured to perform such updates regularly or automatically.

Users must not circumvent or make any attempt to circumvent the administrative, physical and technical safeguards we implement and maintain to protect personal data and the school's ICT facilities.

### 8.3 Data protection

All personal data must be processed and stored in line with data protection regulations and the school's data protection policy, which can be found on the school's website.

### 8.4 Access to facilities and materials

All users of the school's ICT facilities will have clearly defined access rights to school systems, files and devices.

These access rights are managed by the business manager and Head Teacher.

Users should not access, or attempt to access, systems, files or devices to which they have not been granted access. If access is provided in error, or if something a user should not have access to is shared with them, they should alert the Head Teacher immediately.

Users should always log out of systems and lock their equipment when they are not in use to avoid any unauthorised access. Equipment and systems should always be logged out of and closed down completely at the end of each working day except during times where remote access via LgfL's secure access facility, Freedom to Roam is required.

### 8.5 Encryption

The school ensures that its devices and systems have an appropriate level of encryption.

School staff may only use personal devices (including computers and USB drives) to access school data, work remotely, or take personal data (such as pupil information) out of school if they have been specifically authorised to do so by the headteacher.

Use of such personal devices will only be authorised if the devices have appropriate levels of security and encryption, as defined by the Business Manager/Head Teacher.

### 8.6 Saving work securely

All work is to be saved and stored onto the schools G.Drive as this is regularly backed up and saved.

This is in line with the school's business continuity plan and will make sure the school remains operational

## 9. Internet access

The school wireless internet connection is secured.

The school uses London Grid for Learning's filtering system to prevent inappropriate sites from being accessed.

### 9.1 Pupils

Pupils will be given access to Wifi using school ICT equipment. The London Grid for Learning filtering system will be effective on all of these devices ensuring that inappropriate content is not accessed as much as possible.

### 9.2 Parents and visitors

Parents and visitors to the school will not be permitted to use the school's wifi unless specific authorisation is granted by the School. Most Parents working in partnership with the school during their time with us will be granted this permission.

The School will only grant authorisation if:

- Parents are working with the school as part of the Family Model.
- Visitors need to access the school's wifi in order to fulfil the purpose of their visit (for instance, to access materials stored on personal devices as part of a presentation or lesson plan)

Staff must not give the wifi password to anyone who is not authorised to have it. Doing so could result in disciplinary action.

## 10. Monitoring and review

SLT (Senior Leadership Team) will monitor the implementation of this policy, including ensuring that it is updated to reflect the needs and circumstances of the school.

A review of the effectiveness of the school's filtering and monitoring systems will be carried out at least once every academic year by the SLT with the support of the school's DSL and IT support.

This policy will be reviewed annually.

The governing board is responsible for approving this policy.

## 11. Related policies

This policy should be read alongside the school's policies on:

- Safeguarding and child protection
- Behaviour
- Code of Conduct
- Data protection

# The Pears Family Charitable Foundation School

## Appendix 1: Facebook and Social Media cheat sheet for staff (Guidance)

**Don't accept friend requests from pupils or their parents on social media**

### 10 Rules for school staff on Facebook (Guidance)

1. Change your display name – use your first and middle name, use a maiden name, or put your surname backwards instead
2. Change your profile picture to something unidentifiable, or if not, ensure that the image is professional
3. Check your privacy settings regularly
4. Be careful about tagging other staff members in images or posts
5. Don't share anything publicly that you wouldn't be just as happy showing your pupils
6. Don't use social media sites during school hours
7. Don't make comments about your job, your colleagues, our school or your pupils online – once it's out there, it's out there
8. Don't associate yourself with the school on your profile (e.g. by setting it as your workplace, or by 'checking in' at a school event)
9. Don't link your work email address to your social media accounts. Anyone who has this address (or your personal email address/mobile number) is able to find you using this information
10. Consider uninstalling the Facebook app from your phone. The app recognises wifi connections and makes friend suggestions based on who else uses the same wifi connection (such as parents or pupils)

---

### Check your privacy settings

- Change the visibility of your posts and photos to **'Friends only'**, rather than 'Friends of friends'. Otherwise, pupils and their families may still be able to read your posts, see things you've shared and look at your pictures if they're friends with anybody on your contacts list
- Don't forget to check your **old posts and photos** – go to bit.ly/2MdQXMN to find out how to limit the visibility of previous posts
- The public may still be able to see posts you've **'liked'**, even if your profile settings are private, because this depends on the privacy settings of the original poster
- **Google your name** to see what information about you is visible to the public
- Prevent search engines from indexing your profile so that people can't **search for you by name** – go to bit.ly/2zMdVht to find out how to do this
- Remember that **some information is always public**; your display name, profile picture, cover photo, user ID (in the URL for your profile), country, age range and gender

### What do to if…

### A pupil adds you on social media

- In the first instance, ignore and delete the request. Block the pupil from viewing your profile
- Check your privacy settings again, and consider changing your display name or profile picture
- If the pupil asks you about the friend request in person, tell them that you're not allowed to accept friend requests from pupils and that if they persist, you'll have to notify senior leadership and/or their parents. If the pupil persists, take a screenshot of their request and any accompanying messages
- Notify the senior leadership team or the headteacher about what's happening

### A parent adds you on social media

- Decline the offer or ignore the message, consider drafting a stock response to let the parent know that you're doing so.

### You're being harassed on social media, or somebody is spreading something offensive about you

- **Do not** retaliate or respond in any way
- Save evidence of any abuse by taking screenshots and recording the time and date it occurred
- Report the material to Facebook or the relevant social network and ask them to remove it
- If the perpetrator is a current pupil or staff member, our mediation and disciplinary procedures are usually sufficient to deal with online incidents
- If the perpetrator is a parent or other external adult, a senior member of staff should invite them to a meeting to address any reasonable concerns or complaints and/or request they remove the offending comments or material
- If the comments are racist, sexist, of a sexual nature or constitute a hate crime, you or a senior leader should consider contacting the police

# The Pears Family Charitable Foundation School

## Appendix 2: Acceptable use of the internet: agreement for parents and carers

| Acceptable use of the internet: agreement for parents and carers | |
|---|---|
| **Name of parent/carer:**<br><br>**Name of child:** | |
| Online channels are an important way for parents/carers to communicate with, or about, our school.<br>The school uses the following channels:<br>● Email/text groups for parents (for school announcements and information)<br>● Our virtual learning platform (Google Classroom)<br>● ParentMail<br>Parents/carers also set up independent channels to help them stay on top of what's happening in their child's class. For example, class/year Facebook groups, email groups, or chats (through apps such as WhatsApp). | |
| When communicating with the school via official communication channels, or using private/independent channels to talk about the school, I will:<br>● Be respectful towards members of staff, and the school, at all times<br>● Be respectful of other parents/carers and children<br>● Direct any complaints or concerns through the school's official channels, so they can be dealt with in line with the school's complaints procedure<br>I will not:<br>● Use private groups or personal social media to complain about or criticise members of staff. This is not constructive and the school can't improve or address issues if they aren't raised in an appropriate way<br>● Use private groups or personal social media to complain about, or try to resolve, a behaviour issue involving other pupils. I will contact the school and speak to the appropriate member of staff if I'm aware of a specific behaviour issue or incident<br>● Upload or share photos or videos on social media of any child other than my own, unless I have the permission of other children's parents/carers | |
| **Signed:** | **Date:** |

## Appendix 3: Acceptable use agreement for older pupils

| Acceptable use of the school's ICT facilities and internet: agreement for pupils | |
|---|---|
| **Name of pupil:** | |
| **When using the school's ICT facilities and accessing the internet in school, I will not:**<br>● Use them without a teacher being present, or without a teacher's permission<br>● Use them to break school rules<br>● Access any inappropriate websites<br>● Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity)<br>● Use chat rooms<br>● Open any attachments in emails, or follow any links in emails, without first checking with a teacher<br>● Use any inappropriate language when communicating online, including in emails<br>● Share my password with others or log in to the school's network using someone else's details<br>● Bully other people<br>I understand that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.<br>I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others.<br>I will always use the school's ICT systems and internet responsibly.<br>I understand that the school can discipline me if I do certain unacceptable things online, even if I'm not in school when I do them. | |
| **Signed (pupil):** | **Date:** |
| **Parent/carer agreement:** I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these. | |
| **Signed (parent/carer):** | **Date:** |

## Appendix 4: Acceptable use agreement for younger pupils

| Acceptable use of the school's ICT facilities and internet: agreement for pupils | |
|---|---|
| **Name of pupil:** | |
| **When I use the school's ICT facilities (like computers and equipment) and get on the internet in school, I will not:**<br>● Use them without asking a teacher first, or without a teacher in the room with me<br>● Use them to break school rules<br>● Go on any inappropriate websites<br>● Go on Facebook or other social networking sites (unless my teacher said I could as part of a lesson)<br>● Use chat rooms<br>● Open any attachments in emails, or click any links in emails, without checking with a teacher first<br>● Use mean or rude language when talking to other people online or in emails<br>● Share my password with others or log in using someone else's name or password<br>● Bully other people<br>I understand that the school will check the websites I visit and how I use the school's computers and equipment. This is so that they can help keep me safe and make sure I'm following the rules.<br>I will tell a teacher or a member of staff I know immediately if I find anything on a school computer or online that upsets me, or that I know is mean or wrong.<br>I will always be responsible when I use the school's ICT systems and internet.<br>I understand that the school can discipline me if I do certain unacceptable things online, even if I'm not in school when I do them. | |
| **Signed (pupil):** | **Date:** |
| **Parent/carer agreement:** I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these. | |
| **Signed (parent/carer):** | **Date:** |

## Appendix 5: Acceptable use agreement for staff, governors, volunteers and visitors

| Acceptable use of the school's ICT facilities and the internet: agreement for staff, governors, volunteers and visitors | |
|---|---|
| **Name of staff member/governor/volunteer/visitor:** | |
| When using the school's ICT facilities and accessing the internet in school, or outside school on a work device, I will not:<br>● Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)<br>● Use them in any way which could harm the school's reputation<br>● Access social networking sites or chat rooms<br>● Use any improper language when communicating online, including in emails or other messaging services<br>● Install any unauthorised software, or connect unauthorised hardware or devices to the school's network<br>● Share my password with others or log in to the school's network using someone else's details<br>● Share confidential information about the school, its pupils or staff, or other members of the community<br>● Access, modify or share data I'm not authorised to access, modify or share<br>● Promote private businesses, unless that business is directly related to the school | |
| I understand that the school will be able to monitor the websites I visit and my use of the school's ICT facilities and systems.<br>I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.<br>I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.<br>I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too. | |
| **Signed (staff member/governor/volunteer/visitor):** | **Date:** |

## Appendix 6 – Online safety contract Pupils/families

## Online Learning Safety Contract (pupils/families)

# The Pears Family Charitable Foundation School

Whilst we find ourselves back in school and there is less use of online lessons, certain situations might arise when lessons and learning will take place online, there are a few things we ask all of you to do to keep yourselves safe:

- Please be responsible for your own behaviour;
- Please ensure everyone on the meeting is wearing appropriate clothing;
- Everyone MUST respect usual classroom rules – talking respectfully; not using discriminatory language or terms; using appropriate language; not talking over each other;
- Pupils and families must not record the lesson/meeting;
- Try to ensure you are in a space that does not contain personal information;
- Staff will only record meetings/lessons with permission from pupils and families.
- If staff have any concerns about anyone's behaviour online during a lesson, the teacher or staff member will ask them to stop and will terminate the meeting if needed. They will then follow this up with parents and pupil and with the safeguarding lead if required.
- If teachers have concerns about the online safety of the meeting, the meeting will be terminated and the safeguarding lead will be contacted.

By agreeing to this contract we will be able to work with you face to face and stay more connected whilst we are not in school as much.