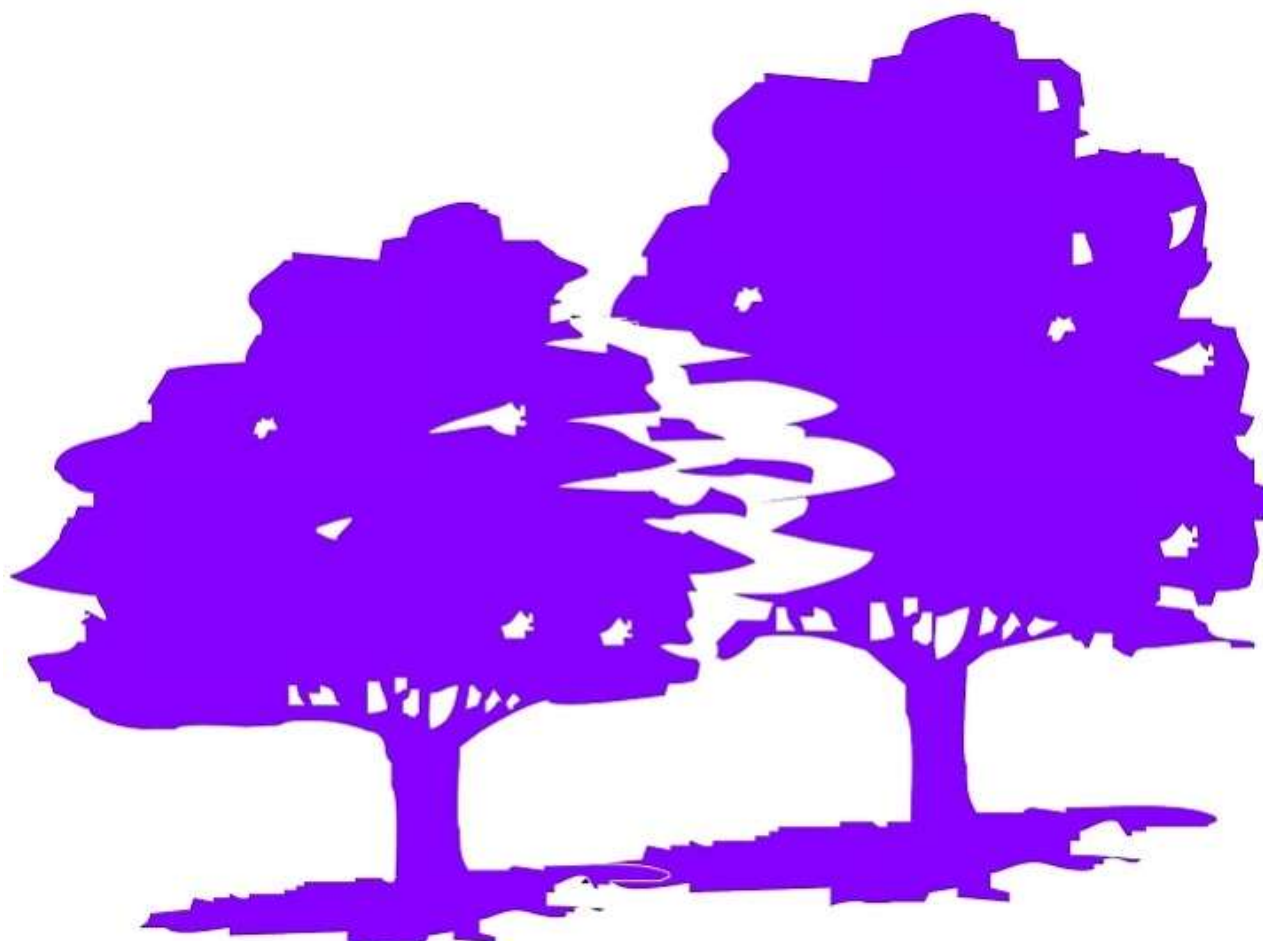


Online safety policy

Tenacres First School



Tenacres

Approved by:

All staff and governors

Date: October 2020

Last reviewed on:

October 2020

Next review due by:

September 2022

Contents

1. Aims	2
2. Legislation and guidance	2
3. Roles and responsibilities	3
4. Educating pupils about online safety	4
5. Educating parents about online safety.....	5
6. Cyber-bullying	5
7. Acceptable use of the internet in school	6
8. Pupils using mobile devices in school	6
9. Staff using work devices outside school	6
10. How the school will respond to issues of misuse	7
11. Training	7
12. Monitoring arrangements	7
13. Links with other policies	7
Appendix 1: EYFS and KS1 acceptable use agreement (pupils and parents/carers).....	8
Appendix 2: acceptable use agreement (staff, governors, volunteers and visitors).....	9
Appendix 3: Laptop Loan Agreement	11
Appendix 4: Social Networking Agreement	13
Appendix 5: Consent form for use of images.....	14
Appendix 6: online safety incident report log	15

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

2. Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, [Keeping Children Safe in Education](#), and its advice for schools on:

- [Teaching online safety in schools](#)
- [Preventing and tackling bullying](#) and [cyber-bullying: advice for headteachers and school staff](#)
- [Relationships and sex education](#)
- [Searching, screening and confiscation](#)

It also refers to the Department's guidance on [protecting children from radicalisation](#).

It reflects existing legislation, including but not limited to the [Education Act 1996](#) (as amended), the [Education and Inspections Act 2006](#) and the [Equality Act 2010](#). In addition, it reflects the [Education Act 2011](#), which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

3. Roles and responsibilities

3.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governor who oversees online safety is **Steph Mann**.

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3)

3.2 The headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The designated safeguarding lead – **Ceri Marshall & DDSL Jeanette Walters / Jon Beacham**

Details of the school's DSL and deputy are set out in our child protection and safeguarding policy as well relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher, ICT coordinator and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board

This list is not intended to be exhaustive.

3.4 The ICT coordinator – **Jon Beacham and technicians Ash Burbridge / Dan Carpenter**

The ICT coordinator is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a monthly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged (see appendix 6) and dealt with appropriately in line with this policy

- › Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- › Maintaining an understanding of this policy
- › Implementing this policy consistently
- › Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 2), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- › Working with the DSL to ensure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- › Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

- › Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- › Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2)

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- › What are the issues? - [UK Safer Internet Centre](#)
- › Hot topics - [Childnet International](#)
- › Parent factsheet - [Childnet International](#)

3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 2).

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum:

The text below is taken from the [National Curriculum computing programmes of study](#).

As of September 2020 Tenacres also follows:

- › [Relationships education and health education](#) in primary schools

In **Key Stage 1**, pupils will be taught to:

- › Use technology safely and respectfully, keeping personal information private
- › Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage 2** will be taught to:

- › Use technology safely, respectfully and responsibly
- › Recognise acceptable and unacceptable behaviour
- › Identify a range of ways to report concerns about content and contact

By the **end of primary school (Year 6 / middle school)**, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not.
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

The safe use of social media and the internet will also be covered in other subjects where relevant.

The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

5. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website & blog or J2E and Seesaw. This policy will also be shared with parents via the website.

Online safety will also be covered during parents' evenings where applicable

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with class teachers and then with safeguarding leads if further support is needed.

Concerns or queries about this policy can be raised with any member of staff or Miss Marshall.

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. **Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)**

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their tutor groups, and the issue will be addressed in assemblies.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

Tenacres also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on [screening, searching and confiscation](#).

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

7. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1-5). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1 -5.

8. Pupils using mobile devices in school

Pupils are not allowed to bring mobile devices into school. However, we have mobile technology such as iPads in school. Children are allowed to use them during:

- Lessons
- Free time as directed by teachers
- Clubs before or after school, or any other activities organised by the school

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see appendices 1 and 2).

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

9. Staff using work devices outside school

See Laptop Loan Agreement for further information.

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 3.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work

device when using it outside school. Any USB devices containing data relating to the school must be encrypted – Tenacres provides these. Laptops are also encrypted to allow staff to work from home.

If staff have any concerns over the security of their device, they must seek advice from Jon Beacham, Ash Burbridge or Dan Carpenter.

Work devices must be used solely for work activities.

10. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies in Behaviour and Acceptable Use Policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

The DSL and DDSL will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 6.

This policy will be reviewed every 2 years by the headteacher and online safety coordinator. At every review, the policy will be shared with the governing board.

13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy

Appendix 1: EYFS and KS1 acceptable use agreement (pupils and parents/carers)







Online Safety guidelines

All pupils at Tenacres First School use computer facilities including Internet access as an essential part of learning. We have filtering, monitoring software and content control to minimise access to inappropriate content via the school network system.

Pupils are given information on Online Safety during PSHE lessons, assemblies and dedicated Computing lessons.

E-mail: Pupils may only use their approved class email accounts on the school network during designated teaching sessions. Teachers will always check the children's emails before they are sent.

Please read the Online Safety rules with your child and then sign to show they have been understood and agreed by you and your child.

- We only use the internet if an adult or grown says we can. 
- We can click on the buttons or links if we think they are safe. 
- We can ask to use the internet in lessons for research. 
- We always ask if we get lost on the Internet. 
- We can send and open friendly emails together only to people we know. 
- We only search for pictures and videos that we need for schoolwork. 
- If we see something that upsets us, we follow these simple steps: turn the screen off, tell an adult and never share or go back!

Consent for Internet Access:

I have read and understood the school e-safety rules and give permission for my child to access the Internet. I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials. I understand that the school cannot be held responsible for the nature or content of materials accessed through the internet. I agree that the school is not liable for any damages arising from use of the Internet facilities.

(parent) Signed: _____ Date: _____

(child) Signed: _____ Date: _____

Social Networking

We trust that you recognise the dangers of discussing school issues on social networking sites and stress the importance of parents/carers supporting the school and raising any concerns directly with us.

Appendix 2: acceptable use agreement (staff, governors, volunteers and visitors)

Background

Technology has transformed learning, entertainment and communication for individuals and for all organisations that work with young people. However, the use of technology can also bring risks. All users should have an entitlement to safe internet access at all times.

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I will, where possible, educate the young people in my care in the safe use of ICT and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (e.g. laptops, email, learning platform) out of the school.
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down in the online safety policy.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
- I will immediately report any illegal, inappropriate or harmful material or incident of which I become aware, to the appropriate person.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital images. I will not use my personal equipment to record these images.
- Where images are published (e.g. on the school website / learning platform) I will ensure that it will not be possible to identify by name, or other personal information, those who are featured. (see section A.3.3 of the online safety policy)
- I will only use chat and social networking sites in school in accordance with the school's policies. (see section A.3.2 of the online safety policy)
- I will only communicate with pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner. (see sections A.3.1 and A.3.2 of the online safety policy)
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- I will only use my personal mobile ICT devices as agreed in the online safety policy (see section A.3.1) and then with the same care as if I was using school equipment. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the school ICT systems except in an emergency (A.3.2).
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.

- I will ensure that my data is regularly backed up in accordance with relevant school policies (Maintained and subscribing establishments see **IBS Schools Systems and Data Security advice**).
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist or radical material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School / LA Personal Data Policy (see e-security policy). **I understand that where personal data is transferred outside the secure school network, it must be encrypted.**
- I will not take or access pupil data, or other sensitive school data, off-site without specific approval. If approved to do so, I will take every precaution to ensure the security of the data,
- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of school:

- I understand that this Acceptable Use Agreement applies not only to my work and use of school ICT equipment in the school, but also applies to my use of school ICT systems and equipment out of the school and to my use of personal equipment in the school or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Agreement, I could be subject to disciplinary action. This could involve a warning, a suspension, referral to Governors and/or the Local Authority and/or other relevant bodies including, in the event of illegal activities, the involvement of the police (see section A.2.6).

I have read and understand the above and agree to use the school ICT systems (both in and out of the school) within these guidelines.

Staff / volunteer Name:	
Signed:	
Date:	

Appendix 3: Laptop Loan Agreement



Tenacres First School Laptop Loan Agreement.



The Headteacher has agreed that a laptop computer will be loaned to you while you remain employed at this school. This loan is subject to review on a regular basis and can be withdrawn at any time.

As a member of staff to whom a laptop has been loaned, I have read and agree to the following terms and conditions that apply while the laptop is in my possession:

- The Laptop and any accessories provided with it, remains the property of Tenacres First School and is strictly for my sole use in assisting in the delivery of the Curriculum. It is not for personal use, e.g. Facebook or other social networking sites or on-line shopping.
- I understand insurance cover provides protection from the standard risks but excludes theft from a vehicle.
- If left unattended the laptop must be securely stored. It must **never** be left unattended even for a short period in a car, including in a locked boot.
- I agree to treat the laptop with due care and keep the laptop in good condition. I will ensure that it is strapped in to the carry case when transported and/or not in use, not leave the laptop unattended in class and avoid food and drink near the keyboard/touch pad.
- I agree to backing up my work on a regular basis. I understand the school will not accept responsibility for the loss of work in the event of the laptop malfunctioning.
- I agree to only use software licensed by the school, authorised by Jon Beacham or our Peritech team.
- I agree that Anti-Virus software is installed and must be updated on a weekly basis. Our Peritech team will advise on the routines and schedule of this operation.
- Should any faults occur, I agree to notify Jon Beacham or the Peritech team as soon as possible so that they may undertake any necessary repairs. Under no circumstances should I, or anyone other than ICT staff, attempt to fix suspected hardware faults.
- I agree to attend training in how to access the Curriculum Network, Intranet, VLE , Internet, and email within the school provided by Jon Beacham, our Peritech team or any outside provides.
- I agree that home Internet access is permitted at the discretion of the Headteacher. I understand the school will not accept responsibility for offering technical support relating to home Internet connectivity.
- I agree that any telephone/broadband charges incurred by staff accessing the Internet from any site other than school premises are not chargeable to the school.
- I agree to adhere to School and LA policies regarding the following, updated as necessary: • Acceptable Use; • Data Protection; • Computer Misuse; • Health and Safety.
- I agree to use a secure password including numbers, uppercase letters and/ or special characters.

Laptop Details

Make	Model	Serial Number

Personnel Details

Loan Authorised by

Headteacher: (signature) Date

I have read and agree to be bound by the terms and conditions set out above.

I agree that my laptop is brought into school **on a Thursday** for regular maintenance.

Name of Member of Staff (Print)

Received by (signature): Date

Note on Insurance

For laptops to be covered automatically under the schools policies at no extra charge, they need to be included on the school's inventory. The standard All Risks insurance policy covers the laptops for theft (where there are signs of forced entry), and accidental or malicious damage. Those Schools who have opted for the additional Buildings and Contents policy will also receive cover for flood/water damage, storm damage etc. All equipment in Schools is automatically covered for fire, lightning and explosion.

Laptops **are not** covered by the school policy: • Whilst in vehicles. Any theft should be immediately reported to the police and a crime reference number should be obtained and provided to the head teacher. If stolen or damaged from an employee's home, County would first ask for a claim under the staff member's household policy. Claims from the School policy will only be made if this were unsuccessful. Please note that regardless of the policy a stolen laptop is claimed under, a claim will not be considered unless there are signs of forced entry or assault.

Appendix 4: Social Networking Agreement

For the protection of yourself, your school community and your establishment:

- Ensure that all your privacy settings are set to 'Friends Only'. Go to your Account Settings and make sure that the Custom Settings are highlighted and that these show that status, photos and posts are set to 'Friends Only'.
- Consider what information you have on your info page and your profile picture. Including brief information and an unidentifiable picture, e.g. sunset, will assist in making your profile indistinctive.
- Be careful what photographs you include on your profile. Once these are uploaded, they are very difficult to remove and, using image editing software, they can be altered and merged with other more distasteful images.
- If you have professional and social 'friends' on Facebook or other social networking sites, using the group list feature will ensure that you can distinguish what type of information you send to particular groups.
- Do not accept pupils (even those that have recently left the school), parents or carers as 'friends'.
- Do not use Facebook or other social networking sites in any way that might bring your professional status or your school into disrepute.
- Taking charge of your digital reputation is important, as unprofessional posts or images will lead to disciplinary action and possible failure to gain employment in the future.
- Do not post or upload photographs relating to colleagues, pupils or parents. Objection to such posts can cause friction in your school and make your working environment uncomfortable.
- Do not post or upload photographs related to school-based or extra-curricular activities and do not make specific reference to your school in any post as comments may be misconstrued and result in inappropriate responses.
- Be aware of any spam or potential virus risks sent via rogue posts. It is advisable to check with anti-virus firms if you get any suspicious requests or posts.
- If you are alerted to any negative or unscrupulous information about yourself, colleagues or your school on Facebook or other social networking sites, inform your headteacher. Further advice to help with cyberbullying incidents etc., can be gained from help@saferinternet.org.uk (0844 3814772) or a professional association such as your Trade Union.
- ***I understand the implications of using Facebook and other social networking sites for my own protection and professional reputation, as well as the impact that my use can have on my school community and establishment.***
- ***I understand that injudicious use of social networking may lead to disciplinary action.***
- ***I agree to take all possible precautions as outlined above.***

Name		Date	
------	--	------	--

Department for Education website (www.education.gov.uk).

Appendix 5: Consent form for use of images



Consent Form for use of Images (photographs, videos, DVDs and digital images)



Photographs and/or video recordings of children may be taken whilst they attend the setting to celebrate their achievements and successes and as evidence of their progress and development. Still or moving images may be published in our printed publications (e.g. prospectus, newsletters) and/or on our external websites. They may also be used to promote the good practice of the setting to other teachers, e.g. at training events organised by the Local Authority or national education/government institutions. Children's names will never be published alongside their photograph externally to the education setting. Names may be used internally, for example – on a display.

Electronic images, whether photographs or videos, will be stored securely on the setting's network which is accessible only by authorised users.

Before using any photographs/videos of your child we need your permission. **Please answer the questions below, then sign and date the form where indicated and return it.**

Please circle

1. May we use your child's photograph in printed publications? **Yes / No**
2. May we use your child's photograph on our internet websites? **Yes/No**
3. May we allow your child's photograph (e.g. as part of a team or record of an event) to be used for publication in a newspaper? *(Please note that the use of photographs in newspapers is subject to strict guidelines)*
Yes / No
4. May we use any photograph or video of your child internally as part of regular activities and work of the setting?
Yes / No
5. May we use any photographs or video containing your child to share good practice with staff from other settings?
Yes / No
6. May we use images of your child on an external web site or for publicity or campaigns by national Government agencies?
Yes/No

This form is valid from the date of signing until your child leaves the setting. Photographs and videos may be securely archived after your child has left the setting. Photographs and videos used for publicity purposes may continue to remain in circulation after your child has left the setting. You may withdraw your consent, in writing, at any time **but it may not be possible to remove images that are already in circulation or have already been published** although every effort will be made to do so.

We recognise that parents, carers and family members will wish to record **their child/ children** at events such as, sports days etc. to celebrate their child's achievements. The setting is happy to allow this, at the discretion of the Headteacher/Senior Manager, on the understanding that such images/recordings are used for purely personal family use. **The Headteacher / Senior Manager will explain when images/recordings may be taken at such events.** Images containing children **other than their own** should not be put on the internet for any reason, without first seeking permission from the other child's parents/carers.

A full copy of the setting's policy on the safe use of children's photographs may be obtained upon request.

Name of Child: Date of birth:

Name of parent / carer:

Signed: Date:

Data Protection Tenacres takes your privacy seriously and we have taken steps to protect it. Any personal data you give to us, including photographic images, will be processed strictly in accordance with the Data Protection Act 1998 and will be used for the purposes that you have consented to. We will not share your details with third parties without your consent, except where we are legally compelled or obligated to do so. Please note that where you consent to images appearing on the internet, they can be viewed worldwide including countries where UK data protection law does not apply.

Appendix 6: online safety incident report log

ONLINE SAFETY INCIDENT LOG				
Date	Where the incident took place	Description of the incident	Action taken	Name and signature of staff member recording the incident