Romans Field School
Bradwell Village School
Priory Common School

INCLUSIVE LEARNING FEDERATION

Online and Acceptable Use Policy

Reviewed by:	**P Outram**
Last reviewed on:	December 2024
Approved at FGB:	5 December 2024
Next review due by:	September 2025

1. Introduction

Information and Communications Technology 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, schools need to build in the use of these technologies in order to prepare our young people with the skills to access life-long learning and employment.

This policy should also be used in line with our Child Protection & Safeguarding Policy.

Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Coding software
- Websites
- Social Media
- Mobile/ Smart phones with text, video, photograph, recording and/ or web functionality
- Other mobile devices with web functionality
- Gaming, especially online
- Learning Platforms and Virtual Learning Environments
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies and that some have minimum age requirements, usually 13 years.

The staff in the Federation understand the responsibility to educate our pupils on Online Safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Schools hold personal data on learners, staff, and other people to help them conduct their day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in media coverage, and potentially damage the reputation of the school. This can make it more difficult for the school to use technology to benefit learners.

In line with the General Data Protection Regulations 2018, everybody in the school has a shared responsibility to secure any sensitive information used in their day-to-day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

2. Roles and Responsibilities

As Online Safety is an important aspect of strategic leadership within the school, the Executive Headteacher and Governors have ultimate responsibility to ensure the policy and practices are embedded and monitored. The Computing Lead is the Online Safety co-ordinator who has been designated this role. All members of the school community have been made aware of who holds this post.

The senior leadership team and governors are updated by the Executive Headteacher and Governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

This policy, supported by the school's acceptable use agreements for staff, governors, visitors, and pupils, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: Child Protection and Safeguarding, Health and Safety, Behaviour, Anti-bullying and PSHE.

3. Online Safety in the Curriculum

ICT and online resources are increasingly used across the curriculum. We believe it is essential for Online Safety guidance to be given to the pupils on a regular and meaningful basis. Online Safety is embedded within our curriculum, and we continually look for new opportunities to promote Online Safety.

- The school provides opportunities within a range of curriculum areas to teach about Online Safety, including the Prevent Duty.
- Educating pupils about the online risks that they may encounter outside school is done informally when opportunities arise and as part of the Online Safety curriculum.
- Pupils are aware of the relevant legislation when using the internet such as data protection and intellectual property rights which may limit what they want to do but also serves to protect them.
- Pupils are taught about copyright, respecting other people's information, and protecting their own personal information, safe use of images and other important areas through discussion, modelling, and appropriate activities.
- Pupils are aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e., parent/carer, teacher/ trusted staff member, or an organisation such as Cybermentors, Childline or CEOP report abuse button.
- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teaching models, discussions and via the Computing curriculum.

4. Pupils with Additional Needs

- The school endeavours to create a consistent message to parents/carers for all pupils and this in turn should aid the establishment and future development of the school's Online Safety rules. However, staff are aware that some pupils may require additional support or teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of Online Safety issues. Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of Online Safety. Internet activities are planned and well managed for these children.

5. E-Mail

The use of e-mail within school is an essential means of communication. In the context of school, e-mail should not be considered private.

- The school gives all staff their own e-mail account to use for all school business as a work-based tool. This is to protect staff, minimise the risk of receiving unsolicited or malicious e-mails and avoid the risk of personal profile information being revealed.
- It is the responsibility of each account holder to keep their password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary, e-mail histories can be traced. The school email account should be the account that is used for all school business.
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal e-mail addresses.
- All e-mails should be written with careful checking of spelling and grammar before sending, in the same way as a letter written on school headed paper.
- Pupils may only use school approved accounts on the school system and only under direct teacher

supervision for educational purposes.

- E-mails created or received as part of your school job will be subject to disclosure in response to a request for information under the Freedom of Information Act. You must therefore actively manage your e-mail account as follows:

  - Delete all e-mails of short-term value
  - Organise e-mail into folders and carry out frequent housekeeping on all folders and archives
- The forwarding of chain letters is not permitted in school.
- Staff must inform (the ICT Technician or Executive Headteacher) if they receive an offensive e-mail whether it is directed at themselves or others and before it is deleted.
- However, you access your school e-mail (whether directly, through webmail when away from the office or on non-school hardware) all the school e-mail policies apply.

Sending E-Mails

- Use your own school e-mail account so that you are clearly identified as the originator of a message.
- Use the school signature at the end of your email, to identify that emails are professional in nature.
- Keep the number and relevance of e-mail recipients, particularly those being copied, to the minimum necessary and appropriate.
- Do not send or forward attachments unnecessarily. Whenever possible, send the location path to the shared drive rather than sending attachments.
- School e-mail is not to be used for personal advertising.

Receiving E-Mails

- Check your e-mail regularly.
- Activate your 'out-of-office' notification when away for extended periods.
- Never open attachments from an untrusted source; consult the ICT Technician first if in doubt.
- Do not use e-mail systems to store attachments. Detach and save business related work to the appropriate shared drive/folder.

6. Online Safety Support for Staff

- Our staff receive regular and appropriate information and training on Online Safety and how they can promote the 'Stay Safe' online messages. This is usually through the usual scheduled programme of staff meetings.
- New staff receive information on the school's acceptable use policy as part of their induction.
- All staff have been made aware of their individual responsibilities relating to the safeguarding of children within the context of Online Safety and know what to do in the event of misuse of technology by any member of the school community.
- All staff are encouraged to incorporate Online Safety activities and awareness within their curriculum areas.

7. The Internet

The internet is an open worldwide communication medium, available to everyone, at all times. Anyone can view information, send messages, discuss ideas, and publish material which makes it both an invaluable resource for education, business, and social interaction, as well as a potential risk to young and vulnerable people. All use of the internet is logged, and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected it will be followed up.

The school provides pupils with supervised access to Internet resources (where reasonable) through the school's wired and Wi-Fi internet connectivity.

Pupils must only access appropriate sites authorised by staff and must report any unacceptable contact to staff

immediately.

Staff will preview any recommended sites before use.

Raw image searches are discouraged when working with pupils.

If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents/carers recheck these sites and supervise this work. Parents/carers will be advised to supervise any further research.

All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.

All users must observe copyright of materials from electronic resources.

On-line gambling or gaming is not allowed.

All staff, volunteers and governors must comply with the Social Networking Policy regarding the posting of any information or images relating to the school.

School internet access is controlled through the internet provider's filtering service.

The Federation is aware of its responsibility when monitoring staff communication under current legislation.

Staff are aware that school-based email and internet activity can be monitored and explored further if required.

If staff or pupils discover an unsuitable site, the screen must be switched off/closed and the incident reported immediately to the ICT Technician.

It is the responsibility of the school to ensure that anti-virus protection is installed and kept up to date on all school machines.

Pupils and staff are not permitted to download programs or files on school-based technologies without seeking prior permission from the ICT Technician.

If there are any issues related to viruses or anti-virus software, the ICT Technician should be informed.

The school does not allow any access to social networking sites.

We believe that it is essential for parents/carers to be fully involved with promoting Online Safety both in and outside of school and to be aware of their responsibilities. We consult and discuss Online Safety with parents/carers and seek to promote a wide understanding of the benefits of new technologies, together with the associated risks.

8. Taking of Images, recordings, and Film

Digital images are easy to capture, reproduce and publish and, therefore, misuse. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness. With the written consent of parents/carers (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment.

- Staff and visitors are not permitted to use **personal** digital equipment, such as mobile phones and cameras, to record images or conversations of pupils, or staff (this includes when on field trips) within the school premises.

- Appropriate images/recordings can be taken using school cameras; these should be transferred as soon as possible to the school's network and deleted from the individual school device.

- Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of pupils, staff, and others without advance permission from the Executive Headteacher.

- Staff must have permission from the Executive Headteacher before any image can be uploaded for publication.

- Where an outside company or individual is commissioned by the school to take images, there must be appropriate DBS clearance and the school should satisfy itself that appropriate arrangements are in place to ensure images are not stored or distributed outside of the school.

9. Publishing Pupil's Images and Work

On a child's entry to the school, all parents/carers will be asked to give permission to use their child's work/photos in the following ways:

- on the school web site;
- in the school prospectus and other printed publications that the school may produce for promotional purposes;
- recorded/ transmitted on a video or webcam;
- in display material that may be used in the school's communal areas;
- in display material that may be used in external areas, i.e., exhibition promoting the school;
- general media appearances, e.g., local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically).

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, e.g., divorce of parents, custody issues, etc. However, it is the practice of the school to ask parents to re-sign this annually at the beginning of each new school year and parents or carers may withdraw permission, in writing, at any time.

Pupils' names will not be published alongside their image and vice versa. Postal addresses of pupils will not be published. Pupils' full names will not be published. Before posting a child's work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed.

10. Storage of Images

- Images/ films of children are stored on the school's network.
- Pupils and staff are not permitted to use personal portable media for storage of images (e.g., USB sticks) without the express permission of the Executive Headteacher or Head of School.
- Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network or other online school resources.

11. Video Conferencing

- Permission is sought from parents and carers if their child is involved in video conferencing.
- All pupils are supervised by a member of staff when video conferencing.
- The school keeps a record of video conferences, including date, time, and participants.
- Approval from the Executive Headteacher is sought prior to all video conferences within school.
- No part of any video conference is recorded in any medium without the written consent of those taking part.

12. Personal Mobile Devices (including phones and Smart Watches)

- The school allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the school allow a member of staff to contact a pupil using their personal device. The personal device is not to be used during contact time with children.
- Staff can only use their mobiles during working hours with the permission of the Executive Headteacher or Head of School.
- The school is not responsible for the loss, damage, or theft of any personal mobile device.
- The sending of inappropriate messages, images (including pseudo images), videos or sounds between any members of the school community is not allowed.
- The creation of inappropriate messages, images (including pseudo images), videos or sounds by any member of the school community is not allowed.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device and do so at their own risk.
- Pupils and parents/carers, visitors are not allowed to use mobile phones on site without the permission of the Executive Headteacher or Head of School.
- Pupils are not allowed to bring Smart Watches to school.

13 Parental/Carer Involvement

- Parents/carers are asked to read through and sign the acceptable use agreements on behalf of their child on admission to the school.
- Parents/carers are required to make a decision as to whether they consent to images of their child being taken and used in the public domain (e.g., on school websites).
- The school disseminates information to parents/carers relating to Online Safety where appropriate in the form of:
    - The school websites
    - Practical training sessions
    - Newsletter items
    - Parent mail

14. Security

The school gives relevant staff access to its Management Information System, with a unique username and password.

- It is the responsibility of everyone to keep passwords secure; passwords are not to be shared with others.
- Staff are aware of their responsibility when accessing school data.
- Staff keep all school-related data secure. This includes all personal, sensitive, confidential, or classified data.
- Staff should avoid leaving any portable or mobile ICT equipment or removable storage media in unattended vehicles. Where this is not possible, keep it locked out of sight and in the boot.
- Staff should always carry portable and mobile ICT equipment or removable media as hand luggage and keep it under your control at all times.
- It is the responsibility of individual staff to ensure the security of any personal, sensitive, confidential, and classified information contained in documents faxed, copied, scanned, or printed.
- All ICT equipment is securely marked as soon as possible after it is received. The ICT Technician maintains a register of all ICT equipment and other portable assets.
- As a user of the school ICT equipment, you are responsible for your activity.
- ICT equipment issued to staff is logged and serial numbers are recorded as part of the school's inventory.
- It is imperative that staff save data on a frequent basis to the school's network. Staff are responsible for the backup and restoration of any of your data that is not held on the school's network.
- Personal or sensitive data should not be stored on the local drives of desktop PC, laptop, USB memory

stick or other portable devices. If it is necessary to do so the local drive must be encrypted. It is recommended that a time-locking screensaver is applied to all machines. Any device accessing personal data must have a locking screensaver as must any user profiles.

- Privately owned ICT equipment should not be used on a school network. On termination of employment, resignation or transfer, staff must return all ICT equipment to the school. Staff must also provide details of all their system logons so that they can be disabled.
- All activities carried out on school systems and hardware will be monitored in accordance with the general policy.
- Equipment must be kept physically secure in accordance with this policy to be covered for insurance purposes. When travelling by car, the best practice is to place the laptop in the boot of your car before starting your journey.
- The installation of any applications or software packages must be authorised by the ICT Technician.
- Portable equipment must be transported in its protective bag.
- Anyone expecting a confidential or sensitive fax should notify the sender before it is sent.

Server Security

- School servers are kept in a lockable store and there are limited access rights to these which are password protected.
- Existing servers have security software installed appropriate to the machine's specification and the school uses a remote back up service and data is backed up daily.

Using Removable Media

- Always consider if an alternative solution already exists.
- Only use recommended removable media.
- Store all removable media securely.
- Removable media must be disposed of securely by the ICT Technician.

Monitoring

- Internet activity is logged by the school's internet provider and in addition the ICT Technician regularly monitors the web sites which are accessed on school equipment.

15 Breaches

A breach or suspected breach of policy by a school employee, contractor or pupil may result in the temporary or permanent withdrawal of school ICT hardware, software, or services from the offending individual.

Any policy breach is grounds for disciplinary action in accordance with the school Disciplinary Procedure. Policy breaches may also lead to criminal or civil proceedings.

16 Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the ICT Technician. Additionally, all security breaches, lost/stolen equipment, or data (including remote access Secure ID tokens and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported.

An incident log is used to monitor what is happening and identify trends or specific concerns. The log is kept securely in the SLT office.

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the ICT Technician.

- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the ICT Technician, depending on the seriousness of the offence; investigation by the Executive Headteacher/ LA, possibly leading to disciplinary action, dismissal, and involvement of police for very serious offences.

17 Protecting Personal, Sensitive, Confidential and Classified Information

Staff will ensure:

- they lock their screen before moving away from their computer during the normal working day to prevent unauthorised access;
- personal, sensitive, confidential, or classified information is not disclosed to any unauthorised person;
- the security of any personal, sensitive, confidential, and classified information contained in documents which are faxed, copied, scanned, or printed;
- only download personal data from systems if expressly authorised to do so by the Executive Headteacher;
- they keep their screen display out of direct view of any third parties when accessing personal, sensitive, confidential, or classified information;
- hard copies of data are securely stored and disposed of after use in accordance with the document labelling;
- they protect school information and data at all times, including any printed material;
- **school laptops and other electronic devices must never be left in an unoccupied car.**

18 Viruses

- All files downloaded from the Internet, received via e-mail or on removable media such as a memory stick must be checked for any viruses using school provided anti-virus software before being used.
- Never interfere with any anti-virus software installed on school ICT equipment that you use.
- If your machine is not routinely connected to the school network, you must make provision for regular virus updates through the ICT Technician.
- If you suspect there may be a virus on any school ICT equipment, stop using the equipment and contact the ICT Technician immediately. The ICT Technician will advise you what actions to take and be responsible for advising others that need to know.

19 Disposal of ICT Equipment

- All redundant ICT equipment will be disposed of through an authorised agency recommended by the LA. This should include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data. Any redundant ICT equipment being considered for sale/gift will have been subject to a recent electrical safety check and hold a valid PAT certificate and if personal data is likely to be held the storage media will be over written multiple times to ensure the data is irretrievably destroyed.
- All redundant ICT equipment that may have held personal data will have the storage media overwritten multiple times to ensure the data is irretrievably destroyed. Or if the storage media has failed it will be physically destroyed.

Disposal of any ICT equipment will conform to current legislation and will conform with the governors' policy on the disposal of equipment.

20 Zombie Accounts

Zombie accounts refer to accounts belonging to users who have left the school and therefore no longer have authorised access to the school's systems. Such Zombie accounts when left active can cause a security threat by allowing unauthorised access.

- The ICT Technician will ensure that all user accounts are disabled once the member of the school has left the school.

21 Remote Learning

Safeguarding and the link to online safety – our ILF Child Protection & Safeguarding Addendum January 2021 states the following:

21.1 In school

We will continue to have appropriate filtering and monitoring systems in place in school.

21.2 Outside school

Where staff are interacting with children online, they will continue to follow our existing staff policy on acceptable use of the internet. Staff will continue to be alert to signs that a child may be at risk of harm online, and act on any concerns immediately, following our reporting procedures as set out in section 3 of this addendum. We will make sure children know how to report any concerns they have back to the relevant school, and signpost them to other sources of support too.

21.3 Working with parents and carers

We will continue to make sure parents and carers:

- are aware of the potential risks to children online and the importance of staying safe online;
- know what our school is asking children to do online, including what sites they will be using and who they will be interacting with from our school;
- know where else they can go for support to keep their children safe online.

This is all done through ParentMail, email and via the website for each school. By 25th January 2021, the remote education programmes for all schools will be available on the individual school's website.

21.4 Using 'Microsoft Teams' or 'Padlet' to communicate internally or externally

Expectations

1. When a pupil is unable to attend school the class team will provide the learning materials through Microsoft Teams/Padlet for all core subjects.
2. Pupils are expected to upload their work into Microsoft Teams/Padlet on a daily basis.
3. staff should, if needed, create instructional teaching videos for difficult to grasp activities.
4. Staff will message pupils through Microsoft Teams/Padlet or via the class email daily to check in on their progress.
5. Staff will agree a weekly video or telephone call with the pupil to talk through any work/issues they have.
6. When video calling a pupil, staff must at all times follow the 'Video Call Good Practice Advice.'
7. All on the call are to be treated with respect and behave with the high expectations expected in a classroom environment.

Video Call Good Practice Advice

When making a video/telephone call you must ensure you follow the advice set out below.

- Before the call
    - Ensure that you have a suitable, quiet place to make the call.
    - Clear the background of the working area of any documents relating to children.

- Remember to plug your laptop in to the mains when making a video call.
- Make sure you are wearing appropriate clothing when making a video call.
- If you have an ID badge you should wear it for a video call.
- Have all resources (note pads etc) nearby to avoid having to leave the area.
- Place a note on the door to avoid being disturbed.
- Close noisy applications such as Outlook to avoid being interrupted.

- During the call
  - Call promptly at the agreed time.
  - Whenever possible have a second member of the staff nearby.
  - Ensure that screen recording is turned on when making a video call.
  - Clearly introduce yourself.
  - Note down anything that concerns or worries you and pass it on to the DSL.

- After the call
  - Take a moment to check through any notes that you have made.
  - Consider if you need to complete any reports following the conversation e.g., cause for concern,
  - Talk to the class team about the call and update relevant staff on the pupil.

Acceptable/Responsible Use Agreement and Safety Rules for Pupils

- I will only use ICT in school for school purposes.
- I will not tell other people my ICT passwords.
- I will only open/delete my own files.
- I will make sure that all ICT contact with other children and adults is responsible, polite, and sensible.
- I will not deliberately look for, save, or send anything that could be unpleasant or nasty. If I accidentally find anything like this, I will tell my teacher immediately.
- I will not give out my own details such as my name, phone number or home address. I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- I will not send photographs or videos or any other information about myself or other children to others.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community
- I know that my use of ICT can be checked and that my parent/carer contacted if a member of school staff is concerned about my Online Safety.

Pupil's Agreement

I have read and I understand the school Rules for Responsible Internet Use. I will use the computer system and Internet in a responsible way and obey these rules at all times. (Parents are asked to read and explain the rules for responsible use with their children.)

Signed: _____ Class: _____

Date: _____

Rules for Responsible Internet Use

Child's Name _____

The school has installed computers and Internet access to help our learning. These rules will keep everyone safe and help us be fair to others.

- I will ask permission from a member of staff before using the Internet.
- I will not access other people's files.
- I will use the computers only for schoolwork and homework.
- I will not bring portable storage items into school unless I have permission.
- I will not give my home address or phone number, or arrange to meet someone, unless my parent, carer or teacher has given permission.
- To help protect other pupils and myself, I will tell a teacher if I see anything I am unhappy with or I receive messages I do not like.
- I understand that the school may check my computer files and may monitor the Internet sites I visit.

Permission for Internet Access	
Parent/carer's permission	***Pupil's agreement***
I give permission for access to the Internet on the terms set out in the above letter.	I agree to follow the Rules for Responsible Internet Use.
Signed: _____ Print name: _____ Date: _____	**Signed: _____** Print name: _____ Date: _____

Acceptable/Responsible Use Agreement for Staff

- I will only use the school's email, internet, network, and any related technologies for professional purposes or for uses defined as 'reasonable' by the Executive Headteacher or Governing Board.

- I will ensure that personal data is kept secure and is used appropriately on school premises. Personal data can only be taken out of school when authorised by the Executive Headteacher.

- I will only use password protected memory sticks and not my own personal devices for storing information.

- I will not install any hardware or software without the permission of the Executive Headteacher or Head of School.

- I am aware that I may use my school laptop for personal use, however I must ensure that at no time this is being used inappropriately or inappropriate material is being accessed – this includes any materials that could be considered offensive, illegal, or discriminatory. I will ensure that my use of ICT is in keeping with the Online Safety Policy.

- I am aware that ICT technical staff monitor the use of ICT and the internet and that if I am found to have been accessing inappropriate material or using ICT inappropriately this may result in disciplinary action being taken.

- If I have any concerns about any incidents where inappropriate pop-ups or other material inadvertently appears I must log this immediately in the ICT incident log and report this to the Executive Headteacher.

- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.

- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.

- I will not give personal details such as mobile phone numbers and personal email addresses to pupils.

- I will support and promote the school's Online Safety Policy and data security and help pupils to be safe and responsible in their use of ICT and related technologies.

- I will ensure that photographs/recordings of children or staff or premises will only be taken with school equipment and where the Executive Headteacher and parents'/carers' /person's/ permissions has been obtained.

- I will ensure that images/recordings of children or staff or premises are not taken or stored on any personal equipment or devices without the permission of my Line Manager.

- I will ensure that I am complying with the Social Networking Policy and that at no time any images or materials are distributed outside the school without the express permission of the Executive Headteacher.

- I will not allow pupils to use my laptop or computer whilst logged on using my password.

- I will keep ICT equipment in the boot of my car when transporting it and I will **never** leave it in the car when it is unoccupied.

Signed: _____ Date: _____