# Glais Primary School

# Policy on Social Media Policy and Use of Mobile Phones and Digital Photography

| | Name | Signature | Date |
|---|---|---|---|
| Chair of Governors | Mr Stuart Page | | |
| Head Teacher | Mrs Anne Long | | |

| | |
|---|---|
| Review Dates<br>(Annual review) | |

## Glais Primary School

## Social Media Policy and Use of Mobile Phones and Digital Photography Policy

Our increasingly digital world plays an important role in the lives of many youngsters. We recognise that this brings risks, but equally there are many benefits to be reaped. The widespread availability and use of digital applications bring opportunities to understand, engage, and communicate in new and exciting ways. It is important that we are able to use these technologies and services effectively and flexibly. However, it is also important to ensure that we balance this with our duties to our school, the community, our legal responsibilities and our reputation. We need to remember that our use of digital applications has implications on our duty to safeguard children and young people.

The policy requirements in this document aim to provide a framework of good practice. They apply to all pupils, parents, visitors, staff and governors at the school.
It is important that all adults set a good example to the children in our school when using these mediums, so that they can grow to be responsible citizens of the future.

This policy should be read in conjunction with other related policies including:
'**CITY & COUNTY OF SWANSEA COUNCIL GUIDANCE ON THE USE OF SOCIAL MEDIA' (Link in Appendix 1); 'GUIDANCE FOR SCHOOLS ON THE SAFE USE OF IMAGES' (Link in Appendix 2); WORKFORCE COUNCIL: GUIDE TO USING SOCIAL MEDIA RESPONSIBLY: (Link in Appendix 3); POLICY FOR SAFE USE OF THE INTERNET (Appendix 4); MOBILE DEVICE ACCEPTABLE USE POLICY (Appendix 5); CITY AND COUNTY OF SWANSEA CODE OF CONDUCT (Appendix 6); CODE OF CONDUCT FOR STAFF (Appendix 7);**

This document gives clarity to the way in which digital applications are to be used at Glais Primary School.

There are six key areas
A. The use of social networking sites within school.
B. Use of social networking by staff in a personal capacity.
C. Comments posted by parents/carers.
D. Dealing with incidents of online bullying.
E. Safeguarding children and the use of digital photography and mobile phones
F. Security and Identity theft

### A. The use of social networking sites within school.

When using social media for educational/promotional purposes, the following practices should be observed:

- The content of any school-sanctioned social media site should be solely professional and should reflect well on the school.

- Staff must not publish photographs of children without the written consent of parents /carers or allow personally identifying information to be published on school social media accounts
- Care must be taken that any links to external sites from the account are appropriate and safe, especially if using remote home access
- Any inappropriate comments on or abuse of school-sanctioned social media should immediately be removed and reported to a member of SLT
- New social media services must be approved by the Headteacher in advance of any educational work being undertaken.
- Staff should be aware that the school may monitor the use of ICT systems, e-mail and other digital communication

**B. Use of social networking by staff in a personal capacity.**
It is possible that a high proportion of staff will have their own social networking site accounts. It is important for them **to protect their professional reputation** by ensuring that they use their personal accounts in an appropriate manner.
Guidelines issued to staff:

1. There is an acknowledgment that school staff may/will have pre-existing engaged communications with parents from the school community. However, school **staff are advised** not to invite, accept or engage in communications with new parents and **should not** accept or engage in communications with children from the school community in any personal social media whilst in employment at Glais Primary School. Those pre-existing communications should be responsible and compliant.
2. Staff must never add pupils or ex pupils under the age of 18 as friends into their personal accounts.
3. Staff must not post pictures of school events without the Headteacher's consent.
4. Staff must not use social networking sites for anything other than professional use within lesson times.
5. Work-based profiles or groups should only be created following agreement by your line manager
6. Staff need to use social networking in a way that does not conflict with the current National Teacher's Standards.
7. Staff should maintain boundaries between their personal and professional lives by customising, reviewing and adjusting their privacy settings to give them the appropriate level of privacy and confidentiality, so preventing inappropriate personal information becoming visible.
8. Staff must not post negative comments about the school, pupils, parents or colleagues including Governors.
9. If any member of staff is aware of inappapropiate communications involving any child in any social media it **must** be reported to the designated person for Child Protection
10. If any member of staff is aware of inappapropiate communications involving any member of the school community they **should** report it to a member of the Leadership team.
11. Staff should read and comply with 'Guidance for Safer Working Practice for Adults who Work with Children and Young People'.

Inappropriate use by staff should be referred to the Headteacher in the first instance or LADO (Local Authority Designated Officer).

**C. Comments posted by parents/carers.**
Parents and carers will be made aware of their responsibilities regarding their use of social networking. Methods of school communication include the prospectus, the website, newsletters, letters and verbal discussion.

1. Parents are not expected to post pictures of pupils other than their own children on social networking sites unless prior permission has been sought from parents of all other pupils in the photograph/video.
2. Parents should make complaints through official school channels rather than posting them on social networking sites.
3. Parents should not post derogatory, malicious or fictitious comments on social networking sites about any member of the school community.

### D. Dealing with incidents of online bullying

Glais Primary School is committed to ensuring that all staff, parents/carers, governors and pupils are treated with dignity and respect. Bullying and harassment of any kind will not be tolerated. The schools e-safety and/or Anti Bullying Policy makes sanctions regarding bullying using new technologies very clear. This indicates that the school can take action against incidents that happen outside school if it:

1. Could have repercussions for the orderly running of the school or
2. Poses a threat to another pupil or member of the public or
3. Could adversely affect the reputation of the school.

Use of social networking sites to harass, bully or intimidate would be covered by this irrespective of when/where the post was made.

### E. Safeguarding of Children

### Use of Mobile Phones and Digital Photography Policy

As this is an area which is integral to the lives of our pupils, within school and outside it, it is important that we ensure that any exposure is properly managed, as improper use could expose both the school and user to potential legal liability.

Children have their photographs taken to provide evidence of their achievements for many purposes, it is however important to be mindful of the following procedures:

1. Under the data protection act of 1998 school must seek parental consent to take photographs and use video recording. The school will send a letter to parents or guardians of pupils, requesting permission. If a parent/guardian **does not** return a non-consent form then permission will be assumed. Photographs will be stored on the school network which is pass word protected until the school ceases to operate, should this occur then all photographs will be shredded or deleted from the school network.
2. The schools digital cameras must not leave the school setting (unless on an educational visit) Photographs are printed in the setting by staff and images are then removed from the camera by staff.
3. Photographs may be taken during indoor and outdoor play and learning and displayed in school sanctioned media e.g. prospectus, website, books. Often photographs may contain other children in the background.
4. Events such as Sports Day, outings, Christmas and fundraising events may be recorded by video and photographs by staff and parent/carers but always in full view of all attending. Parents must not post photographs or video containing other children on social media websites without prior permission. (See Policy above).
5. On occasion the school might like to use photographs of children taking part in an activity to advertise/promote the school via the website etc, however in this instance, the permission slips will indicate whether this is acceptable.
6. Many mobile phones have inbuilt cameras so staff mobile phones must not be used to take pictures of children in our school. **Visitors may only use their phones in the foyer or outside the building and should be challenged if seen using a camera inappropriately or photographing children. Pupils are not allowed to use their phones in school and must leave them in the office.**
7. The use of cameras and mobile phones are prohibited in toilets and changing areas.
8. Staff are asked not to make personal calls during their working hours. However in urgent cases a call may be made or accepted if deemed necessary and by arrangement with the Headteacher.
9. All school cameras and recording devices should be kept securely at all times and used with appropriate authority. **Staff, visitors, volunteers and students are not permitted to use their own mobile phones to take or record any images of school children for their own records during the school day unless prior permission has been granted for specific purposes.**

### F. Security and Identity Theft

Staff, governors, parents and carers should be aware that social networking websites are a public forum, particularly if they are part of a ‘network’. Staff, governors, parents and carers should not assume that their entries on any website will remain private.
Staff, governors, parents and carers must also be security conscious and should take steps to protect themselves from identity theft, for example by restricting the amount of personal information that they give out. Social networking websites allow people to post detailed personal information such as date of birth, place of birth and, for example, favourite football team which can form the basis of security questions and passwords.
It is vital that everyone takes steps to ensure that anything that is posted is protected and only accessible by those it was intended for.

The Headteacher may seek legal advice on any matters related to the potential misuse of digital media and may consider any breaches a disciplinary matter.

Glais Primary 2015

**Appendix 1**

http://www.learn- ict.org.uk/intsafety/documents/swan_ docs/Social_Media_ Guidelines. pdf

**Appendix 2**

http://www.learn-ict.org.uk/intsafety/documents/swan_docs/Use_of_Images.pdf

**Appendix 3**

http://www.ewc.wales/site/images/documents/fitness_to_practise/Using_Social_Media.pdf

**Appendix 4**

## Glais Primary School

## A Policy for Acceptable Use of Internet and E-mail

This policy has been written with close regard to the LEA Guidelines & School’s Acceptable Use Policy. This policy is intended to protect the interests of the users in their use of the Internet and e-mail.

**The Internet and e-mail facility should not be used for transmitting or receiving material which is:-**

- Illegal, obscene, offensive, fraudulent, etc
- Discriminatory (on the grounds of race, gender, nationality, culture, religion, sexual orientation, age, disability or personal characteristics).
- Defamatory – including libellous and slanderous comments.
- An intrusion into other people’s privacy, or which may be construed as harassing them.
- In breach of copyright (it is illegal to download or copy material without prior permission of the owner, furthermore, copyright in material exists automatically, and no statement to this effect is required).

- In contravention of the Data Protection Act (using personal data for unauthorised purpose).
- Confidential information.

**Do not use the Internet or e-mail facility for:-**

- Chain letters
- Private business use or personal advertisements
- Chat lines or playing games other than those linked to the curriculum
- Online betting or gambling
- Newsgroups, bulletin boards, mailing lists other than those recognised for the use within the curriculum – these must be authorised either by a member of staff or the headteacher. (These are areas where names and addresses are made available to a wider audience and as such could result in junk mail (SPAM) causing overloading of mailboxes and wasted time).

**In addition to the above, the following must be adhered to:**

- Users must not make their known their Ids or passwords to other users
- No user shall utilise another user's ID or password to access systems
- No user shall access another user's e-mail without their express authorisation.
- No user shall send e-mail from another user's PC, or from a PC where another user is currently logged in, without their express authorisation.

This Policy should be read in conjunction with other related policies

**Review** This policy will be reviewed as appropriate

**Appendix 5**

## Glais Primary School

## Mobile Device Acceptable Use Policy

The policies, procedures and information within this document applies to all iPads, iPod Touches or any other IT handheld or mobile device used in school. Teachers and other school staff may also set additional requirements for use within their classroom.

### Users Responsibilities

Users must use protective covers/cases for their iPad.

The iPad screen is made of glass and therefore is subject to cracking and breaking if misused: Never drop nor place heavy objects (books, laptops, etc.) on top of the iPad.

Only a soft cloth or approved laptop screen cleaning solution is to be used to clean the iPad screen.

Do not subject the iPad to extreme heat or cold.

Do not store or leave unattended in vehicles.

Users may not photograph any other person, without that persons' consent.

The iPad is subject to routine monitoring by Glais Primary School. Devices must be surrendered immediately upon request by any member of staff.

Users in breach of the Responsible Use Policy may be subject to but not limited to; disciplinary action, confiscation, removal of content or referral to external agencies in the event of illegal activity.

Glais Primary School is not responsible for the financial or other loss of any personal files that may be deleted from an iPad.

**Additional Responsibilities for Pupils**

If an iPad is left at home or is not charged, the user remains responsible for completing all schoolwork as if they had use of their iPad.

Pupils must not use their iPad in School corridors on their journeys to and from school or outside of School buildings (unless with the Teachers' permission).

Pupils in breach of the Responsible Use Policy may be subject to but not limited to; disciplinary action, confiscation, removal of content or referral to external agencies in the event of illegal activity.

**Safeguarding and Maintaining as an Academic Tool**

iPad batteries are required to be charged and be ready to use in school so need to be returned in the morning.

Syncing the iPad to iTunes or iCloud will be maintained by a School administrator.

Items deleted from the iPad cannot be recovered.

The whereabouts of the iPad should be known at all times.

It is a user's responsibility to keep their iPad safe and secure,

**Lost, Damaged or Stolen iPad**

If the iPad is lost, stolen, or damaged, the Head Teacher must be notified immediately. iPads that are believed to be stolen can be tracked through iCloud. **<u>You will be liable for a replacement if due care has not been taken.</u>**

**Prohibited Uses (not exclusive):**

**<u>iPads must not be used at home to access the internet.</u>**

Accessing Inappropriate Materials – All material on the iPad must adhere to the ICT Responsible Use Policy. Users are not allow to send, access, upload, download or distribute offensive, threatening, pornographic, obscene, or sexually explicit materials.

Illegal Activities – Use of the school's internet/e-mail accounts for financial or commercial gain or for any illegal activity.

Violating Copyrights – Users are not allowed to have music and install apps on their iPad.

Cameras – Users must use good judgment when using the camera. The user agrees that the camera will not be used to take inappropriate, illicit or sexually explicit photographs or videos, nor will it be used to embarrass anyone in any way. Any use of camera in toilets or changing rooms, regardless of intent, will be treated as a serious violation.

Images of other people may only be made with the permission of those in the photograph.

Posting of images/movie on the Internet into a public forum is strictly forbidden, without the express permission of the Teacher or in the case of staff use; a member of the Senior Leadership team.

Use of the camera and microphone is strictly prohibited unless permission is granted by a teacher.

Misuse of Passwords, Codes or other Unauthorized Access: Users are encouraged to set a passcode on their iPad to prevent other Users from misusing it.

Any user caught trying to gain access to another user's accounts, files or data will be subject to disciplinary action.

Malicious Use/Vandalism – Any attempt to destroy hardware, software or data will be subject to disciplinary action.

Jailbreaking – Jailbreaking is the process of which removes any limitations placed on the iPad by Apple. Jailbreaking results in a less secure device and is strictly prohibited.

Inappropriate media may not be used as a screensaver or background photo. Presence of pornographic materials, inappropriate language, alcohol, drug or gang related symbols or pictures will result in disciplinary actions.

Individual users are responsible for the setting up and use of any home internet connections and no support will be provided for this by the school.

Users should be aware of and abide by the guidelines set out by the School eSafety policy.

Glais Primary School reserves the right to confiscate and search an iPad to ensure compliance with this Responsible Use Policy.

**Parents must read and sign below:**

I have read, understand and agree to abide by the terms of the iPad

Acceptable Use Policy.

Name__________________________ Signature_______________________ Date________________

Please read the iPad Acceptable Use Policy below:

**Student Pledge for iPad Use**

I will take good care of my iPad.

I will never leave the iPad unattended.

I will never lend my iPad to others.

I will know where my iPad is at all times.

I will return my ipad in the morning to charge the battery

I will keep food and drinks away from my iPad since they may cause damage

to the device.

I will not disassemble any part of my iPad or attempt any repairs.

I will protect my iPad by only carrying it whilst it is in a case.

I will use my iPad in ways that are appropriate.

I understand that my iPad is subject to inspection at any time without notice.

I will only photograph people with their permission.

I will only use the camera or the microphone when my teacher tells me to.

I will never share any images or movies of people in a public space on the

Internet, unless I am asked to do so by my Teacher.

I agree to abide by the statements of this iPad acceptable use policy

Name_____________________________________ Date________________________

Mobile Device Acceptable Use Policy *Glais Primary School 2012*

Appendix 6

## City and County of Swansea
## Code of Conduct Policy

Introduction

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. These technologies can stimulate discussion, promote creativity and make learning more effective. They also bring opportunities for staff to make learning more engaging and data management more efficient. However, the school is aware that improper use of these systems could expose both the school and the user to potential legal liability. The school will endeavour to ensure that staff and volunteers have good access to ICT to enhance their work and the learning opportunities for pupils in their care. In return the school expects staff and volunteers to agree to be responsible users of ICT.

This Acceptable Use Policy is intended to ensure that:

- staff and volunteers will be responsible users of ICT and stay safe while using the Internet and other communications technologies for educational, personal and recreational use;
- school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk;
- staff are protected from potential risk in their use of ICT in their everyday work.
- for professional and personal safety:

the school may monitor my use of the ICT systems, email and other digital communications;

- the rules set out in the agreement also apply to use of school ICT systems (e.g. laptops, email, the Swansea-Edunet Learning Platform) outside the school and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones, camera phones, PDAs and portable media players, etc.)

**Passwords**

- Always use your own personal passwords to access computer based services.
- Make sure you enter your personal passwords each time you logon. Do not include passwords in any automated logon procedures.
- Change your password whenever there is any indication of possible system or password compromise.
- Do not record your passwords or encryption keys on paper or in an unprotected file.
- Only disclose your personal password to authorised ICT support staff when necessary, and never to anyone else. Ensure that all personal passwords that have been disclosed are changed once the requirement is finished.
- Make sure that logged-on workstations are not left unattended.

**Remote Access**

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

- Only use equipment with an appropriate level of security for remote access.
- To prevent unauthorised access to school systems, do not disclose your username and password to anyone.
- Select passwords that are not easily guessed e.g. do not use your house or telephone number or choose consecutive or repeated numbers.
- Avoid writing down or otherwise recording any network access information. Any such information that is written down must be kept in a secure place and disguised so that no other person will be able to identify what it is.
- Protect school information and data at all times, including any printed material produced while using the remote access facility. Take particular care when access is from a non-School environment.

**Storing/Transferring Personal, Sensitive, Confidential or Classified Information Using Removable Media**

- Ensure removable media is purchased with built-in encryption systems.
- Store all removable media securely.
- Securely dispose of removable media that may hold personal data.
- Encrypt all files containing personal, sensitive, confidential or classified data.
- Ensure hard drives from machines no longer in service are removed and stored securely or wiped clean.

**School ICT Equipment including Portable & Mobile ICT Equipment & Removable Media**
**School ICT Equipment**

- As a user of ICT, you are responsible for any activity undertaken on the school's ICT equipment provided to you.
- Ensure that all ICT equipment that you use is kept physically secure.
- It is imperative that you save your data on a frequent basis to the school's network drive. You are responsible for the backup and restoration of any of your data that is not held on the school's network drive.
- Personal or sensitive data should not be stored on the local drives of desktop PCs. If it is necessary to do so the local drive must be encrypted.
- Privately owned ICT equipment should not be used on a school network.
- On termination of employment, resignation or transfer, return all ICT equipment to your Manager. You must also provide details of all your system logons so that they can be disabled.
- It is your responsibility to ensure that any information accessed from your own PC or removable media equipment is kept secure, and that no personal, sensitive, confidential or classified information is disclosed to any unauthorised person.

**Mobile Technologies**

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Many existing mobile technologies such as portable media players, PDAs, gaming devices, mobile and Smart phones are familiar to children outside of school too. Emerging technologies will be examined for educational benefit and the risk assessed before their use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

**Personal Mobile Devices (including phones)**

- 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 or parent/carer using their personal device.
- This technology may be used, however for educational purposes, as mutually agreed with the Headteacher. The school is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate text messages between any members of the school community is not allowed.
- Permission must be sought before any images or sound recordings are made on these devices of any member of the school community.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

**School Provided Mobile Devices (including phones)**

- The sending of inappropriate text messages between any members of the school community is not allowed.
- Permission must be sought before any images or sound recordings are made on the devices of any member of the school community.
- Where the school provides mobile technologies such as phones, laptops and PDAs for offsite visits and trips, only these devices should be used.
- Where the school provides a laptop for staff, only this device may be used to conduct school business outside of school.

**Guidance for staff on the use of Social Networks & Blogs**

Social networking sites (e.g. Facebook, MySpace etc.) and blogging sites (e.g. Wordpress, Twitter etc.) are a way of life for many young people and adults. However, adults working with children should review their use of social networks as they take on professional responsibilities. Once published online, information such as photographs and blogs are almost impossible to control. Some adults have been 'caught out' by posting comments or remarks about work or colleagues. It is strongly advised that you make no reference to your school life on these sites or otherwise bring your employer into disrepute.

**Safe Use of Images**

(For advice see the: **Guidance for Schools on Safe Use of Images**. (http://www.learn-ict.org.uk/intsafety/index.asp)

**Passwords**

- Always use your own personal passwords to access computer based services.
- Make sure you enter your personal passwords each time you logon. Do not include passwords in any automated logon procedures.
- Change your password whenever there is any indication of possible system or password compromise.
- Do not record your passwords or encryption keys on paper or in an unprotected file.
- Only disclose your personal password to authorised ICT support staff when necessary, and never to anyone else. Ensure that all personal passwords that have been disclosed are changed once the requirement is finished.
- Make sure that logged-on workstations are not left unattended.

**Remote Access**

- You are responsible for all activity via your remote access facility.
- Only use equipment with an appropriate level of security for remote access.
- To prevent unauthorised access to school systems, do not disclose your username and password to anyone.
- Select passwords that are not easily guessed e.g. do not use your house or telephone number or choose consecutive or repeated numbers.
- Avoid writing down or otherwise recording any network access information. Any such information that is written down must be kept in a secure place and disguised so that no other person will be able to identify what it is.
- Protect school information and data at all times, including any printed material produced while using the remote access facility. Take particular care when access is from a non-School environment.

**Storing/Transferring Personal, Sensitive, Confidential or Classified Information Using Removable Media**

- Ensure removable media is purchased with built-in encryption systems.
- Store all removable media securely.
- Securely dispose of removable media that may hold personal data.
- Encrypt all files containing personal, sensitive, confidential or classified data.
- Ensure hard drives from machines no longer in service are removed and stored securely or wiped clean.

### Safe Use of Images

(For advice see the: **Guidance for Schools on Safe Use of Images**. (http://www.learn-ict.org.uk/intsafety/index.asp)

### School ICT Equipment including Portable & Mobile ICT Equipment & Removable Media

### School ICT Equipment

- As a user of ICT, you are responsible for any activity undertaken on the school's ICT equipment provided to you.
- Ensure that all ICT equipment that you use is kept physically secure.
- It is imperative that you save your data on a frequent basis to the school's network drive. You are responsible for the backup and restoration of any of your data that is not held on the school's network drive.
- Personal or sensitive data should not be stored on the local drives of desktop PCs. If it is necessary to do so the local drive must be encrypted.
- Privately owned ICT equipment should not be used on a school network.
- On termination of employment, resignation or transfer, return all ICT equipment to your Manager. You must also provide details of all your system logons so that they can be disabled.

- It is your responsibility to ensure that any information accessed from your own PC or removable media equipment is kept secure, and that no personal, sensitive, confidential or classified information is disclosed to any unauthorised person.

### Mobile Technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Many existing mobile technologies such as portable media players, PDAs, gaming devices, mobile and Smart phones are familiar to children outside of school too. Emerging technologies will be examined for educational benefit and the risk assessed before their use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

### Personal Mobile Devices (including phones)

- 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 or parent/carer using their personal device.
- This technology may be used, however for educational purposes, as mutually agreed with the Headteacher. The school is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate text messages between any members of the school community is

**Appendix 7**

## Staff Acceptable Use Agreement / Code of Conduct

• I will only use the school's e-mail/Internet/Intranet/Learning Portal and any related technologies for professional purposes or for uses deemed 'reasonable' by the Headteacher or Governing Body.

• 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 out my own personal details, such as mobile phone number and personal e-mail address, to pupils.

• I will only use the approved, secure e-mail system(s) for any school business.

• I will ensure that personal data (such as data held on MIS software) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body. Personal or sensitive data taken off site must be encrypted.

• I will not install any hardware or software without the permission of the Network Manager.

• I will not browse, download, upload or distribute any material that could be considered offensive, illegal, defamatory or discriminatory.

• Images of pupils and/or staff will only be taken, stored and used for professional purposes in-line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/carer, member of staff or Headteacher.

• I understand that my use of the Internet and other related technologies may be monitored and logged and can be made available, on request, to my Line Manager or Headteacher.

• I will respect copyright and intellectual property rights.

• I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute and any concerns I have will be brought to the attention of the leadership team.

• I will support and promote the school's e-Safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies.

**User Signature**
I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school.

**Signature** ……..……………………..………… **Date** ……………………

**Full Name** ………………………………........................................

**Job title** . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .