

Our E-safety policy has been written by the school, based on guidance from SWGFL. It has been agreed by the Senior Leadership Team and approved by governors. It will be reviewed annually.

Date: _____

To be revised: _____

Signed _____



E-Safety Policies

This policy uses guidance from SWGFL E-Safety Template. Listed below is legislative framework under which this E-Safety Policy template and guidance has been produced.	
Computer Misuse Act 1990	Data Protection Act 1998
Communications Act 2003	Freedom of Information Act 2000
Malicious Communications Act 1988	Regulation of Investigatory Powers Act 2000
Copyright, Designs and Patents Act 1988	Trade Marks Act 1994
Telecommunications Act 1984	Sexual Offences Act 2003
Criminal Justice & Public Order Act 1994	Public Order Act 1986
Racial and Religious Hatred Act 2006	Obscene Publications Act 1959 and 1964
Protection from Harassment Act 1997	Human Rights Act 1998
Protection of Children Act 1978	The Education and Inspections Act 2011
The School Information Regulations 2012	The Protection of Freedoms Act 2012
Related school policies are listed below	
Behaviour Policy	Anti-Bullying Policy
Computing Policy 2014	

Staff (and Volunteer) Acceptable Use Policy Agreement

New technologies have become integral to the lives of children in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

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

The school will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for pupils learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

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 recognise the value of the use of ICT for enhancing learning and will ensure that pupils receive opportunities to gain from the use of ICT. I will, where possible, educate the children in my care in the safe use of ICT and embed e-safety in my work with children.

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, school website) out of school, and to the transfer of personal data (digital or paper based) out of 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 by the school.
- 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 understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident I become aware of 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 / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Images which are published will only be identifiable by a first name.
- I will only communicate with pupils and parents / carers using official school systems. Emails sent will be from the school's own email address. There will be no occurrences of any communication with pupils / parents / carers over social media sites or through text messaging. Any such communication will be professional in tone and manner.

- I will not engage in any on-line activity that may compromise my professional responsibilities.
- When I use my mobile devices (PDAs / laptops / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I were using school equipment. I will also follow any additional rules set by the school about such use. 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 my mobile phone to email, text or make calls in work time
- I will not use personal email addresses on the school ICT systems to communicate with pupils and parents / carers.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (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
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist 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 Personal Data Policy (or other relevant policy). Paper based Protected and Restricted data must be held in a secure place.
- 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 school 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) See Copyright licence.

Staff should **NOT** make use of internet sites for personal interests during their specified working hours.

- When accessing internet sites staff must use their own username and password.
- When accessing internet sites all staff must adhere to the Staff Acceptable Use Policy.

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

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, referral to Governors and / or the Local Authority or a suspension and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Social Networking Policy for staff and volunteers

Social Network Sites (SNS) have become a significant part of life for many people. Examples of SNS include: Facebook, MySpace, Bebo, You Tube, MSN, online gaming and chatrooms.

Staff are expected to keep a professional distance from pupils and parents and there should be a clear separation of the private lives of staff and pupils and parents. It is important that staff are able to use technologies and services effectively and flexibly, whilst ensuring that they do not make themselves vulnerable.

Aims of the policy:

- Enable staff to use social networking sites safely and securely
- Ensure staff are aware of the risks associated with inappropriate use of social networking sites
- Safeguard staff in the use of social networking sites to ensure they do not make themselves vulnerable to abuse or accusation
- Ensure the school is not exposed to legal risks
- Ensure the reputation of the school is not adversely affected
- Ensure the Governing Body maintains its duty to safeguard children, the reputation of the school, the wider community and the Local Authority.

The Governing Body will ensure this policy is implemented and will provide all staff access to the policy. The Head Teacher and Senior Leadership Team will:

- Ensure all staff thoroughly understand the rules
- Provide information to volunteers and students to ensure they adhere to staff rules relating to use of social media (verbal and written)
- Make staff aware of the risks and possible implications of the inappropriate use of social networking sites
- Instigate appropriate disciplinary procedures where necessary

All staff have a duty to:

- Behave and act responsibly and professionally at all times in the use of social networking sites. They should acknowledge that anything said, shown or received via such sites could be made available, intentionally or otherwise to an audience not originally intended
- Co-operate with the Governing body fully in the implementation of the policy
- Social networking applications are banned from personal use in work time
- Uploading inappropriate photographs or indecent comments on any social network sites is prohibited. Staff should avoid language which could be deemed as offensive to others
- Pupils (past or present) are forbidden to be spoken to as friends on any social network sites until they reach the age of 18. This personal communication is considered unprofessional and inappropriate as well as leaving staff vulnerable to allegations
- No reference to the school, Local Authority, members of staff (colleagues) or pupils should be ever disclosed whether they are positive or negative
- In **no** circumstances should photographs of pupils be posted on social network sites other than the school website (following school guidance)
- Legitimate conversations between staff and parents should not breach any school confidences.

Staff are not discouraged from using social media, however they must be aware that the Governing Body will take seriously and take necessary action where the guidelines set out in this policy have not been followed. It is important that staff remember during their use of SNS, that they reflect their positive conduct and professionalism. If occasions arise of what could be deemed to be online bullying or harassment, these will be dealt with in the same strict manner. The Regulation of Investigatory Powers Act 2000 RIPA permits the Head Teacher the right to monitor the school users internet access. If such monitoring detects inappropriate/unauthorised use of social networking sites, disciplinary action will be taken. The Head Teacher will take seriously any allegations of inappropriate use of social networking sites that are disclosed. There may be instances where the School or Local Authority is obliged to inform the police if there are concerns as to its legality.

Mobile Phone Policy

Staff must keep their mobile phone in: their own staff locker (preferred option) or the Staffroom, however this will be at Staff's own risk as there can be no guarantee of safety. During this time all phones must be on 'silent' or switched off.

There may be extreme circumstances (eg. acutely sick relative) when a member of staff will have requested permission from the Head Teacher to carry their phone in case of having to receive an emergency call. However, this will be kept in 'silent' mode. In the Head Teacher's absence authorisation must be requested from the Deputy Head Teacher. Preferably any emergency calls should use the school number.

During playtimes and lunchtimes when staff are **not** on duty, staff are permitted to use their mobile phones.

It is not deemed appropriate to share images or information of a sexualised nature, or anything that would make another member of staff feel uncomfortable at seeing/hearing the content of a phone call, text or picture message. Content of this nature is only to be shared in personal time when **off** school premises.

All staff must be aware that they adhere to the Staff Acceptable Use policy and no infringements are made that could bring them or the school into disrepute.

iPad Acceptable Use Policy Staff Responsibilities

- Staff 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 on show in vehicles
- When using the iPad to record photographs/video, the Staff Acceptable Use policy should be followed
- The iPad is subject to routine monitoring by the Head Teacher. Devices must be surrendered immediately upon request by the Head Teacher
- Staff 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.
- No personal files of a sensitive nature should be stored on an iPad as children will have access to these throughout the day
- Staff are responsible for keeping their iPad safe and secure

Safeguarding and Maintaining as an Academic Tool

Staff use of the school's iPads should be work related and include no content of a sensitive nature.

- iPad batteries are required to be charged and be ready to use in school
- Syncing the iPad to iTunes or iCloud will be maintained by a school technician
- Items deleted from the iPad cannot be recovered
- Memory space is limited. Academic content takes precedence over personal files and apps
- The whereabouts of the iPad should be known at all times
- iPads belonging to other Staff are not to be tampered with in any manner
- If an iPad is found unattended, it should be given to Business Manager

Prohibited Uses:

- Accessing Inappropriate Materials – All material on the iPad must adhere to the Staff Acceptable Use Policy
- Staff are not allow to send, access, upload, download or distribute offensive, threatening, pornographic, obscene, or sexually explicit materials
- Violating Copyrights – All app installations must receive authorisation from the School Technician or ICT Co-ordinator
- Cameras – Staff 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 prior permission of those in the photograph.
- Posting of images/movie on the Internet into a public forum is strictly forbidden
- Misuse of Passwords, Codes or other Unauthorised Access: Staff are encouraged to set a password on their iPad and should refer to Acceptable Use Policy regarding confidentiality of passwords
- 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 Staff are responsible for the setting up and use of any home internet connections and no support will be provided for this by the school
- Staff should be aware of and abide by the guidelines set out by the School E Safety policy.

Lost, Damaged or Stolen iPad

If the iPad is lost, stolen, or damaged, the IT Technician /Head Teacher must be notified immediately as iPads that are believed to be stolen can be tracked through iCloud

School Personal Data Handling Policy

Schools and their employees should do everything within their power to ensure the safety and security of any material of a personal or sensitive nature

It is the responsibility of all members of the school community to take care when handling, using or transferring personal data so that it cannot be accessed by anyone who does not:

- have permission to access that data, and/or
- need to have access to that data.

Data breaches can have serious effects on individuals and / or institutions concerned, can bring the school into disrepute and may well result in disciplinary action, criminal prosecution and fines imposed by the Information Commissioners Office, for the school and the individuals involved. Particularly, all transfer of data is subject to risk of loss or contamination.

Anyone who has access to personal data must know, understand and adhere to this policy, which brings together the legal requirements contained in relevant data protection legislation and relevant regulations and guidance.

The school will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for. Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay. All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".

Personal Data

The school and individuals will have access to a wide range of personal information and data. The data may be held in a digital format or on paper records. Personal data is defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances. This will include:

- Personal information about members of the school community – including pupils, members of staff and parents / carers e.g. names, addresses, contact details, legal guardianship contact details, health records, disciplinary records
- Academic data e.g. class lists, pupil progress records, reports, references
- Professional records e.g. employment history, taxation and national insurance records, appraisal records and references
- Any other information that might be disclosed by parents / carers or by other agencies working with families or staff members.

The school's Senior Information Risk Officer (SIRO) is our Business Manager, who will keep up to date with current legislation and guidance and will determine and take responsibility for the school's information risk policy and risk assessment.

The school Information Asset Owners (IAOS) are the Business Manager and Data Protection Officer. The IAOs will manage and address risks to the information and will understand:

- What information is held, for how long and for what purpose,
- How information has been amended or added to over time, and
- Who has access to protected data and why.

Everyone in the school has the responsibility of handling protected or sensitive data in a safe and secure manner.

Governors are required to comply fully with this policy in the event that they have access to personal data, when engaged in their role as a Governor.

The school is registered as a Data Controller on the Data Protection Register held by the Information Commissioner.

Information to Parents / Carers – the “Privacy Notice”

In order to comply with the fair processing requirements of the DPA, the school will inform parents / carers of all pupils of the data they collect, process and hold on the pupils, the purposes for which the data is held and the third parties (e.g. LA, DfE, etc) to whom it may be passed. Parents / carers will be informed about how data is collected and held in the school's prospectus and in the induction evenings for new parents.

Secure Storage of and access to data

Documents of highest security are held on the G Drive and access to this is restricted by password and location. Other data is held on the T Drive school network which is accessible by password. Staff are encouraged to either change their password or determine if their password has been breached at least annually.

The School Technician monitors the automatic backing up, accessing and restoring all data held on school systems, including off-site backups.

All paper based Protected and Restricted (or higher) material is held in lockable storage.

The school recognises that under Section 7 of the DPA, data subjects have a number of rights in connection with their personal data, the main one being the right of access. Procedures are in place to deal with Access Requests by the Business Manager.

Secure transfer of data and access out of school

All sensitive data is transferred via the G Drive and school email by authorised members of staff only.

Pupil records completed through SPTO are accessible by staff only using secure passwords.

Disposal of data

The school will comply with the requirements for the safe destruction of personal data when it is no longer required.

The Business Manager has the responsibility to dispose of data, paper based and electronic copies, related to the latest safety guidelines.

School Technical Security Policy (including filtering and passwords)

Effective technical security depends not only on technical measures, but also on appropriate policies and procedures and on good user education and training. The school will be responsible for ensuring that the school network is as safe and secure as is reasonably possible and that:

- Users can only access data to which they have right of access
- Access to personal data is securely controlled in line with the school's personal data policy

The management of technical security will be the responsibility of School Technician.

Technical Security

The school will be responsible for ensuring that the school network is as safe and secure as is reasonably possible within the framework of SWGFL.

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- Appropriate security measures are in place to protect the servers, firewalls, switches, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.
- Responsibilities for the management of technical security are clearly assigned to appropriate and well trained staff – School Technician
- All users will have clearly defined access rights to school technical systems.
- Users will be made responsible for the security of their username and password and must not allow other users to access the systems using their log on details without clear permission given and must immediately report any suspicion or evidence that there has been a breach of security.
- The Business Manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations supported by the I.T co-ordinator and I.T Technician.
- Mobile device security and management procedures are in place
- Users can report any actual / potential technical incident to the Head Teacher
- Password protected access for approved visitors to have temporary access whilst on site
- Staff are required to keep removable media (USB) secure when taking off site
- The school infrastructure and individual workstations are protected by up to date software to protect against malicious threats from viruses, worms, and trojans by School Technician.

Password Security

A safe and secure username / password system is essential if the above is to be established and will apply to all school technical systems, including networks, devices and email.

- All users will have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the Business Manager
- All school networks and systems will be protected by secure passwords that are regularly changed
- The “master / administrator” passwords for the school systems, used by the technical staff must also be available to the Head Teacher and kept in a secure place e.g. school safe.
- Passwords for new users, and replacement passwords for existing users will be allocated by School Technician

Username and Passwords

- All staff users will be provided with a username and password
- Each class has a unique username and password for pupils

Members of staff will be made aware of the school's password policy on induction to school, by reading and understanding the school's E-Safety policy and Password Security policy, and Acceptable Use Agreement (AUP) Pupils will be made aware of the school's password policy through the Acceptable Use Agreement (read and understood by parent/carer).

School Technician will ensure that full records are kept of:

- User Ids/log ons and requests for password changes
- Security incidents related to this policy

Filtering

The school security and filtering systems are supported by SWGFL.

Electronic devices

An authorised member of staff finding an electronic device will hand it to the Head Teacher.

If inappropriate material is found on the device it is up to the Head Teacher to decide whether they should delete that material, retain it as evidence (of a criminal offence or a breach of school discipline) or whether the material is of such seriousness that it requires the involvement of the police. Examples of illegal activity would include:

- Child sexual abuse images (including images of one child held by another child)
- Adult material which potentially breaches the Obscene Publications Act
- Criminally racist material
- Other criminal conduct, activity or materials

Deletion of Data

If inappropriate material is found on the device, it is up to the Head Teacher to decide whether they should delete that material, retain it as evidence (of a possible criminal offence or a breach of school discipline) or whether the material is of such seriousness that it requires the involvement of the police. A record will be kept of the reasons for the deletion of data / files.

Care of Confiscated Devices

The Head Teacher will ensure that full records are kept of incidents involving the searching for and of mobile phones and electronic devices and the deletion of data / files.

Parent / Carer Acceptable Use Agreement

Digital technologies have become integral to the lives of children, both within schools and outside school. These technologies provide powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Children should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- That children will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- That school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- That parents and carers are aware of the importance of E-safety and are involved in the education and guidance of children with regard to their on-line behaviour.

The school will try to ensure that children will have good access to digital technologies to enhance their learning and will, in return, expect the agreement to be responsible users.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

Permission

As the parent / carer of the above pupil above I give permission for my son / daughter to have access to the internet and to ICT systems at school.

I understand that the school will discuss the Acceptable Use Agreement with my son / daughter and that they will receive, E-safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that children will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's / daughter's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy. I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's E-safety.

Pupil Name Signature of Parent/Carer Date

Pupil Acceptable Use Policy Agreement for Children in Foundation, Year One and Year Two

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers
- I will only use activities that a teacher or suitable adult has told or allowed me to use.
- I will take care of the computer and other equipment
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have made a mistake.
- I will tell a teacher or suitable adult if I see something that upsets me on the screen.
- I know that if I break the rules I might not be allowed to use a computer.

Signed (Parent / Carer):

Date

Guidelines for the use of Digital / Video images

The use of digital / video images plays an important part in learning activities. Pupils and members of staff may use digital cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons.

Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media. By signing this form you are giving permission for us to use your child's image. Children will only be identifiable by their first name. The school will comply with the Data Protection Act.

In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use. To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images.

Digital / Video Images Permission Form

Parent / Carers Name

Pupil Name

- As the Parent / Carer of the above pupil, I agree to the school taking and using digital / video images of my child / children. I understand that the images will only be used to support learning activities or in publicity that reasonably celebrates success and promotes the work of the school.
- I agree that if I take digital or video images at, or of, – school events which include images of children, other than my own, I will abide by these guidelines in my use of these images.

Signature of Parent/ Carer

Date

Staff name		Date	
Staff Acceptable Use Policy (and E Safety Policies)	I have read and understand the guidelines in this policy and agree to follow these.		
Social Networking Policy	I have read and understand the guidelines in this policy, and agree to safe and responsible use of social media to protect and safeguard myself and the school from allegations.		
Mobile Phone Policy	I have read and understand the guidelines in this policy, and agree to safe and responsible use of my mobile phone during my working hours and when on school premises.		

Staff name		Date	
Staff Acceptable Use Policy (and E Safety Policies)	I have read and understand the guidelines in this policy and agree to follow these.		
Social Networking Policy	I have read and understand the guidelines in this policy, and agree to safe and responsible use of social media to protect and safeguard myself and the school from allegations.		
Mobile Phone Policy	I have read and understand the guidelines in this policy, and agree to safe and responsible use of my mobile phone during my working hours and when on school premises.		

Staff name		Date	
Staff Acceptable Use Policy (and E Safety Policies)	I have read and understand the guidelines in this policy and agree to follow these.		
Social Networking Policy	I have read and understand the guidelines in this policy, and agree to safe and responsible use of social media to protect and safeguard myself and the school from allegations.		
Mobile Phone Policy	I have read and understand the guidelines in this policy, and agree to safe and responsible use of my mobile phone during my working hours and when on school premises.		

Staff name		Date	
Staff Acceptable Use Policy (and E Safety Policies)	I have read and understand the guidelines in this policy and agree to follow these.		
Social Networking Policy	I have read and understand the guidelines in this policy, and agree to safe and responsible use of social media to protect and safeguard myself and the school from allegations.		
Mobile Phone Policy	I have read and understand the guidelines in this policy, and agree to safe and responsible use of my mobile phone during my working hours and when on school premises.		