GORSE RIDE SCHOOLS

GROW | RESPECT | SUCCEED

ONLINE SAFETY POLICY

ADOPTED :	September 2019
DATE OF LAST REVIEW :	September 2020
REVIEWED BY :	Governing Body / Executive Head Teacher
DATE OF NEXT REVIEW :	September 2021

ONLINE SAFETY POLICY

CONTENTS

INTRODUCTION

This policy should be read in conjunction with national standards and other relevant local and school policies, procedures and guidelines, e.g.

- Teachers' Standards (DfE, 2012) [available here]
- Wokingham Model Safeguarding Policy (updated May 2018) [available here]
- Safeguarding/Child Protection including the DfE Keeping Children Safe in Education statutory guidance
- Data Protection (GDPR) / Freedom of Information
- Discipline/Behaviour
- Teaching & Learning
- Complaints Procedure
- Staff Handbook

RECORD OF DOCUMENT CHANGES

Section	Change
All	New Online Safety Guidelines developed from the Wokingham 'All in One' e-Safety Guidelines v3.8.1
1	Roles and responsibilities updated in line with Keeping Children Safe in Education (2020) to show that the DSL is overall responsible for Online Safety.
Appendix 3	Parent/Carer support for Student/Pupil Acceptable Use Agreement edited to clarify school responsibility in the event of inappropriate content being identified.

ROLES AND RESPONSIBILITIES

Governors

Governors are responsible for the approval of the Online Safety Policy (including Acceptable Use Agreements), ensuring that it is implemented and reviewing its effectiveness. In fulfilling this responsibility, the governing body may choose to appoint an Online Safety governor and establish an Online Safety committee with appropriate representation. Governors will undertake the following regular activities:

- Meetings with the member of staff responsible for online safety.
- Monitoring of online safety incident logs.
- Reporting to relevant governor committees.
- Keeping up to date with school online safety matters.

Head Teacher

The Head Teacher is responsible for ensuring the overall safety, including online safety, of members of the school community. The Designated Safeguarding Lead (DSL) holds a responsibility for online safety as part of their role (as noted in the 2020 Keeping Children Safe in Education statutory guidance). On a practical day to day basis, the Online Safety Co-ordinator (Computing Subject Leader) along with the Network Manager hold this responsibility. However, the Head Teacher will ensure the following:

- Staff with online safety responsibilities receive suitable and regular training enabling them to carry out their online safety roles and to train other colleagues as necessary.
- The Senior Leadership Team (SLT) receives regular monitoring reports.
- There is a clear procedure to be followed in the event of a serious online safety allegation being made against a member of staff.

Online Safety Co-ordinator (Computing Subject Leader)

As noted above, the Designated Safeguarding Lead holds a responsibility for online safety as part of their role (as noted in the 2020 Keeping Children Safe in Education statutory guidance). The school may opt to appoint an Online Safety Co-ordinator to assist the DSL in their duties. The Online Safety Co-ordinator in turn work will with the IT technician and our IT Support company to ensure that policies are put into practice. The specific duties of the Online Safety Co-ordinator include:

- Take a leading role in establishing and reviewing the school's Online Safety Policy and associated documents.
- Provide materials and advice for integrating online safety within schemes of work and check that online safety is taught on a regular basis.
- Liaise with the school's Designated Safeguarding Lead.
- Liaise with the school's IT technical staff.
- Ensure that online safety incidents are reported and logged and used to inform future online safety developments.
- Report to the governors and meet with them as required.
- Report regularly to the SLT.

IT Technician/Support Provider

The IT Technician/Support Provider is responsible for ensuring that all reasonable measures have been taken to protect the school's network(s). This will involve ensuring the following:

- The IT infrastructure is secure and protected from misuse or malicious attack.
- The school meets the online safety technical requirements outlined in any relevant online guidance.
- Users may only access the school's network(s) through a properly enforced password protection policy.
- The school's filtering policy is applied and updated as appropriate.
- Any inappropriate use of the school's computer systems should be reported to the appropriate senior person.
- Provide secure external access to the school network as appropriate.

Teaching and Support Staff

Teaching and support staff are responsible for ensuring that:

- They are familiar with current online safety matters and the school's Online Safety Policy and practices.
- They have read and understood the school's Staff Acceptable Use Policy (AUP) and signed to indicate agreement.
- They report any suspected misuse or problem to the Online Safety Co-ordinator for investigation and action.
- Electronic communications with pupils should be on a professional level and only carried out using approved school IT systems.
- Online safety issues are embedded in all aspects of the curriculum and other school activities.
- Pupils understand and follow the school's Online Safety and Acceptable Use Policies.

- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations in relation to their age.
- They monitor IT activity in lessons, extra-curricular and extended school activities.
- They are aware of online safety issues related to the use of mobile phones, cameras and handheld devices and that they monitor their use and implement school policies with regard to these devices.
- They know and follow the procedure for dealing with any unsuitable material that is found in internet searches.

Designated Safeguarding Lead (DSL)

The DSL holds the responsibility for online safety as part of their role (as noted in the 2020 Keeping Children Safe in Education statutory guidance). They are trained in online safety issues and be aware of child protection matters that may arise from any of the following:

- Sharing or loss of personal data
- Access to illegal/inappropriate materials
- Inappropriate online contact with adults/strangers
- Potential or actual incidents of grooming
- Cyberbullying
- Provide training and advice for staff and ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.

Data Protection Officer (DPO)

The DPO has a related role which is detailed in Data Protection policies and related documentation.

REVIEWING, REPORTING AND SANCTIONS

Review

- This policy will be reviewed and updated annually, or more often if necessary.
- The school will audit provision to establish if the Online Safety Policy is adequate and that its implementation is effective.

Acceptable Use Agreements

- All users of school IT equipment will sign the appropriate Acceptable Use Agreement. This includes all staff and pupils.
- Parents may be asked to sign on behalf of their children or to show agreement with and support for the school's policy.

[See *'Appendix 3 – Exemplar Acceptable Use Agreements'* for further information]

Reporting and logging

- The school will produce clear guidelines as to what should be done if inappropriate content is found when accessing the internet.
- Any such occurrence will be logged for review and any necessary actions that arise.
- All pupils and teachers should be aware of these guidelines.

[See *'Appendix 1 – Course of action if inappropriate content is found'* for further information]

Complaints regarding internet use

- Any complaints relating to internet misuse should be made in accordance with the school's existing complaints procedure.

- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

Sanctions

- Failure to comply with the requirements of this policy will be dealt in line with the school's existing policies on behaviour, rewards and sanctions.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 or other related legislation. This would constitute a disciplinary matter in the case of staff.

COMMUNICATIONS & COMMUNICATION TECHNOLOGIES

Mobile phones and personal handheld devices

- Infant Pupils will not be allowed to bring mobile phones to school and only Year 6 pupils are permitted if prior arrangements are made with the school.
- Where mobile phones are allowed in school they must be handed into the main school office prior to the beginning of the school day. They will be stored in a class box and pupils are responsible for collection at the end of the school day. Mobile phones may not be used during lessons or formal school time. The sending of abusive or inappropriate text messages or images is forbidden. COVID-19 update: Currently pupils are not permitted to take mobile phones to school as they cannot be stored securely without contamination.
- Pupils will not be allowed to bring in games devices, particularly those which allow ad hoc networks to be established.
- Teacher/parent contact should normally be by the main school telephone and not via a mobile device except where off-site activities dictate the use of a mobile phone.
- Parent helpers in school and staff must ensure that they do not send personal messages, either audio or text, during contact time with pupils. If an exceptional emergency arises they should arrange temporary cover whilst they make a call.
- Staff and pupils may send educational messages during lesson times if these are part of the curriculum.
- Schools should be particularly vigilant where mobile phones may be used with children in Foundation Stage. Staff, helper and visitor mobile devices should normally be switched off or to silent mode during the times that children are present.
- No device in any school building should contain any content that is inappropriate or illegal.
- Identified staff will be given permission to carry mobile phones where they are supporting pupils in an area not in close proximity to other staff and the pupil has a history of absconding or violent tendencies.

E-mail and messaging

- Pupils and staff will be informed that the use of school e-mail or messaging accounts may be monitored.
- Pupils should report any receipt of an offensive e-mail or message on school IT systems.
- Pupils should not reveal details of themselves or others, such as address or telephone number, or arrange to meet anyone via an e-mail or message.
- Information of a sensitive nature should not be sent by unencrypted e-mail.

Social networking

For the purpose of this policy social networking is considered to be any digital media or medium that facilitates interaction.

- Staff use of social networking should be compatible with their professional role and show the highest standards of integrity.
- Pupil use of social networking should conform to age restrictions.

[See *'Appendix 2 – Social Networking Guidance'* for further information]

Internet usage

- Pupils and staff will be informed that internet access will be monitored.
- The school will take all reasonable precautions to ensure that users access only appropriate material. Whilst it is not possible to guarantee that unsuitable material will never appear on a school computer the school will take appropriate measures to prevent a reoccurrence, including contacting the service provider.
- Users must not create, download, upload, display or access knowingly, sites that contain pornography or other unsuitable material that might be deemed illegal, obscene or offensive.
- Unauthorised users must not attempt to disable, bypass or reconfigure any filtering, virus protection or similar.
- All pupils using the internet, and associated communication technologies, will be made aware of the school's online safety guidelines. These should be posted near to the computer systems.
- Pupils will receive guidance in responsible and safe use on a regular basis

Digital and video images

Parental permission

- The school will ensure that, where appropriate, consent is obtained for the taking and use of digital and video images of pupils. Such use could include the school website or social media; display material in and around the school or off site; the school prospectus or other printed promotional material; local/national press.
- Pupils will not be identified by name in any title or commentary accompanying digital or video images that is in the public domain, unless specific parental consent has been obtained.
- Where parental permission has not been obtained, or it is known that a pupil should not be photographed or filmed, every reasonable effort should be made to ensure that a pupil's image is not recorded.

Storage and deletion

- Images should be uploaded to a secure location that is the control of the school. Where memory cards, USB drives, CDs or cloud storage are used during the process of capture or transfer, users should ensure that these are deleted and cleared from any temporary storage or recycle bins.
- Images should be deleted in line with the school's procedures on data retention and disposal.

Recording of images

- School digital devices should always be used to record images of pupils (subject to any variation the school agrees as noted below in 'Use of staff personal devices').
- All pupils appearing in images should be appropriately dressed.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- All digital devices capable of taking photographs and recording sound or video, whether belonging to the school or personal, may be subject to scrutiny if required.
- Where volunteers are supporting school staff, they should abide by the same rules as school staff.

Use of staff personal devices

It is recognised that the most straightforward approach is not to allow use of staff personally owned devices (e.g. staff smartphones, personally owned cameras) to record images. Where this is not possible e.g. for off-site activities, the following apply:

- It will be clearly understood under what circumstances it is permissible to use a personal device.
- Images will be transferred to a secure location on the school's system as soon as possible and the originals/any copies fully deleted.
- Such staff personal devices should be passcode protected.

Parents taking photographs or video

Where the school allows the recording of images at 'public' events the following apply:

- Images may only be recorded for personal use and can only be shared with family and friends. They must not be shared on social networking sites or other websites that are accessible by the general public.

Events/Activities involving multiple schools

- When taking part in events organised by other schools or organisations, e.g. sports or music events, the schools involved will consider what image guidelines should apply.
- For larger events specific image guidelines will be in place and should include reference to press images where relevant.
- Consideration will be given as to how those attending the event will be informed of the image guidelines that apply, e.g. a letter before the event, announcement at the event, or information in any printed programme.
- Although the school will make reasonable efforts to safeguard the digital images of pupils, parents should be made aware that at some types of event it is not always realistic to strictly enforce image guidelines. The school cannot therefore be held accountable for the use of images taken by parents or members of the public at events.

INFRASTRUCTURE AND SECURITY

Security

The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that procedures outlined within this policy are implemented by those responsible.

- School IT technical staff may monitor and record the activity of users on the school IT systems and users will be made aware of this.
- Servers, and communications cabinets should be securely located and physical access restricted.
- Wireless systems should be appropriately secured.
- All users will have clearly defined access rights to school IT systems.
- Access to the school IT systems will cease when a pupil leaves or, in the case of a member of staff, ceases to be employed by the school.
- Appropriate procedures are in place for secure storage and access to 'Administrator' passwords.

Passwords

All staff are provided with an individual password. Pupils have an individual password for accessing the network where possible, though group password may be used for young children.

School advise staff on the choice and use of passwords. The following is advised:

- 'Strong' passwords should be used.
- No individual should tell another individual their password.
- No individual should log on using another individual's password, unless they are a member of staff logging on as a pupil for sound educational or technical reasons.
- Once a computer has been used, users must remember to log off.
- Users leaving a computer temporarily should lock the screen (Windows key + L on a PC).

Filtering

The school maintains and supports the managed filtering service provided by RM Education, the Internet Service Provider (ISP)

- Changes to network filtering should be approved by the appropriate person(s).
- Any filtering issues should be reported immediately to the ISP.

Virus protection

- All computer systems, including staff laptops/devices, are protected by an antivirus product which is administered centrally and automatically updated.

Staff laptops/devices and flash drives

Where staff laptops/devices and flash drives are to be taken out of school, it is possible that they may contain sensitive data, therefore all such devices and removable media are encrypted.

The following security measures have been taken with staff laptop/mobile devices:

- Laptops/devices must be out of view and preferably locked away overnight whether at school or home.
- Laptops/devices should not be used for purposes beyond that associated with the work of the school, e.g. by the family of a member of staff.
- Where others are to use the laptop, they should log on as a separate user without administrator privileges.

[See *'Appendix 3 – Exemplar Acceptable Use Agreements'* for further information]

Data protection

See Data Protection Policy for specific guidance in relation to the security of personal data.

Electronic devices - search and deletion

Schools have the power to search pupils for items 'banned under the school rules' and the power to 'delete data' stored on seized electronic devices. Clear guidelines relating to this is communicated to staff and parents. This includes:

- Items which are banned under the school rules and may be searched for include mobile phones; tablets, i-pods, i-pads, 3DS and similar devices
- All staff members are authorised to examine and/or erase data on electronic devices
- When searching a pupil another member of staff must be present; there will be no physical contact; the search will be conducted away from other pupils.
- Screen shots may be taken as evidence of inappropriate use or witness statements
- Incidents will be reported to the Head Teacher, DSL and/or Online safety Co-ordinator and recorded on an alert form if a child protection issue or in the usual manner if considered to be a bullying issue.

ONLINE SAFETY EDUCATION

Learning and teaching for pupils

- Pupils are encouraged to adopt safe and responsible use of IT, the internet and mobile devices both within and outside school.
- Pupils are helped to understand the need for an Acceptable Use Policy and asked to sign to indicate agreement.
- Pupils are taught to be critically aware of the materials/content they access online and are guided to validate the accuracy of information.
- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Key online safety messages are included within the curriculum and reinforced as part of a planned programme of assemblies and other appropriate opportunities.
- Rules for the use of computers/devices are displayed in all rooms and displayed next to fixed site computers.

Staff training

- Staff are kept up to date through regular online safety training.
- Staff should always act as good role models in their use of IT, the internet and mobile devices.

Parental support

The support of, and partnership with, parents is encouraged through the following:

- Awareness of the school's policies regarding online safety and internet use; and where appropriate being asked to sign to indicate agreement.
- Practical demonstrations and training
- Advice and guidance on areas such as:
    - filtering systems
    - educational and leisure activities
    - suggestions for safe internet use at home

APPENDIX 1 – COURSE OF ACTION IF INAPPROPRIATE CONTENT IS FOUND

- If inappropriate web content is found (i.e. that is pornographic, violent, sexist, racist or horrific) the user should:
  - Turn off the monitor or minimise the window.
  - Report the incident to the teacher or responsible adult.
- The teacher/responsible adult should:
  - Ensure the well-being of the pupil.
  - Note the details of the incident, especially the web page address that was unsuitable (without re-showing the page to the pupils).
  - Report the details of the incident to the Online Safety Co-ordinator.
- The Designated Safeguarding Lead, Online Safety Co-ordinator or other appropriate person will then:
  - Log the incident and take any appropriate action.
  - Where necessary report the incident to the Internet Service Provider (ISP) so that additional actions can be taken.

APPENDIX 2 – SOCIAL NETWORKING GUIDELINES

Staff conduct

- Staff will always conduct themselves with the highest standards of professional integrity and be aware that how they as individuals are perceived in the virtual world may reflect on how the school is perceived.
- Staff should give careful consideration when posting personal information as to how this might be viewed by pupils and parents, even when the postings are within a 'private' online space.

Access to social networking sites

- Social networking sites should never be accessed during timetabled lessons and other contact with pupils and not normally during school working hours.
- Staff may not use school equipment to access social networking sites.
- If the school chooses to make 'official' use of social networking sites this should only be by authorised individuals.

Posting of images and/or video clips

- Photographic images and/or movie clips of children at the school or past pupils, up to the age of 18, should never be posted unless specific consent has been obtained.
- Photographic images and/or movie clips of school staff should not be posted unless specific consent has been obtained.

Privacy

- Staff should recognise that their existing lists of friends/contacts/followers may include people who are part of both their private and professional lives.
- Staff should never be online 'friends' with children at the school or past pupils up to the age of 18.
- Staff should not create new links with parents at the school, unless there is a professional reason for doing so. In such instances there should be a clear understanding of the purpose of the link and what 'information' the parent will have access to.
- Profile settings should be regularly checked, and updated as necessary, to ensure that posted comments and images are not publicly accessible.
- Any changes to social networking sites and privacy settings should be clearly understood.

APPENDIX 3 – ACCEPTABLE USE AGREEMENT

The exemplars included are:

- Student/Pupil Acceptable Use Agreement
- Parent/Carer support for Student/Pupil Acceptable Use Agreement
- Exemplar Laptop Acceptable Use Agreement
- Staff Acceptable Use Agreement

ACCEPTABLE USE AGREEMENT - PUPILS

This document is intended for all KS1 pupils (Reception, Year 1 and Year 2) and their parents/carers.

KS1 E-Safety Agreement – keeping me safe at home and at school

If I see something or read something that makes me feel worried or unhappy or upset, I will tell a grown up straight away

If I get stuck or lost on the internet I will ask a grown up for help

I will always send polite and friendly messages

I will only send messages to people I know

I will keep my personal information (my name, my address, my school) secret and not share it online

KS1 E-Safety Agreement - Pupil Declaration

Child's Name:		Class :	
Parent Signature:		Date:	

Parent/Carer support for Pupil Acceptable Use Agreement

As the parent/carer of the above pupil, I confirm that I, with my child, have read and discussed Gorse Ride Schools Acceptable Use Agreement.

I am confident that my son/daughter has understood the importance of online safety and this agreement.

I understand that my son/daughter will have access to the internet and to IT systems at school. I am aware that this activity will be monitored for safety and security reasons to safeguard both my child and the schools' systems. This monitoring will take place in accordance with data protection and human rights legislation.

I know that my child has received, or will receive, online safety education to help them understand the importance of safe use of IT – both in and out of school.

I understand that the school will take every reasonable precaution, including filtering systems, to ensure that young people will be safe when they use the internet and IT systems. I also understand that although internet filtering systems usually work very well, inappropriate content may occasionally still be accessible, but in this instance the school will take appropriate action with the service provider to request such content is removed.

I fully support the school's online safety approaches and will encourage my child to adopt safe use of the internet and digital technologies at home.

I will inform the school if I have any concerns over my child's, or any other members of the school community's online safety.

I know that I can visit the following websites for further information about keeping my child safe online.

- www.thinkuknow.co.uk/parents
- www.internetmatters.org
- www.saferinternet.org.uk
- www.childnet.com

ACCEPTABLE USE AGREEMENT - PUPILS

This document is intended for all KS2 pupils (Years 3 – 6) and their parents/carers.

KS2 E-Safety Agreement

For my own personal safety:

- I will ask permission from a member of staff before using the Internet at school.
- I will only use the Internet when a responsible adult is in the room.
- I am aware of 'stranger danger' when online and will not meet online friends in real life.
- I will not tell anyone my username or password nor will I try to use any other person's username and password.
- I will not give out any personal information (e.g. full name, home address, telephone number, birthday, school) about myself or anyone else when online that could be used to identify me, my family or my friends unless a trusted adult has given permission.
- I will not arrange to meet people offline that I have communicated with online.
- I will be very careful when sharing pictures or videos of myself or my friends and if I am at school I will always check with a teacher first. I know that once a picture has been shared it cannot be deleted – however silly or embarrassing it is.
- I will only play video games that are suitable for my age.
- I am aware that some websites and social networking sites have age restrictions and I should respect these.
- If I receive a message that upsets me or makes me feel uncomfortable, I will not respond to it or delete it and I will immediately show it to a teacher or responsible adult so it can be traced back to the sender.
- I will immediately report any unpleasant or inappropriate material or anything that makes me feel uncomfortable when I see it online.

Respecting everyone's rights to use technology as a resource:

- I understand that the school IT systems are primarily intended for educational use and that I will not use the systems for personal or recreational use unless I have permission to do so.
- I will not use the school IT systems for online gaming, online gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube).

Acting as I expect others to act toward me:

- The messages I send will be polite and responsible.
- I will respect others' work and property and will not access, copy, remove or otherwise alter anyone else's files, without the person's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I respect that others may have different opinions.
- I will not take or share images of anyone without their knowledge and permission.

Keeping secure and safe when using technology in school:

- I will only use approved e-mail or message accounts on the school system.
- I will not use my personal handheld/external devices (e.g. mobile phones, USB devices, etc.) in school.
- I will only use the school's computers for schoolwork and homework.
- I will not try to upload, download or access any materials or files which are illegal or inappropriate or may cause harm or distress to others or which may be harmful to the school's IT systems
- I will immediately report any damage or faults involving equipment or software.
- I will not open any attachments to e-mails, unless given permission to do so and I know and trust the person/organisation that sent the e-mail.
- I will ask for permission before sending an e-mail to an external person/organisation
- I will not try to bypass the system to reach websites or apps that the school has blocked
- 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.
- I will immediately tell a staff member if I receive an offensive e-mail or message.
- I understand that the school will monitor my use of the IT systems, e-mail and other digital communications when at school.

Using the internet for research or recreation:

- When I am using the internet to find information, I should take care to check that the information that I access is accurate.
- I should 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 try to download copies (including music and videos).

Taking responsibility for my actions, both in and out of school:

- I understand that the school may take action against me if I am involved in incidents of inappropriate behaviour whether this is inside or outside of school. If the activities are illegal, this may be reported to the police.
- I understand that if I break these rules I will be subject to disciplinary action as outlined in the school's Behaviour Policy. This may also include loss of access to the school network/internet.

KS2 E-Safety Agreement - Pupil Declaration

I have read and understood the above and agree to follow the rules outlined.

Name:		Class :	
Signature:		Date:	

Parent/Carer support for Pupil Acceptable Use Agreement

As the parent/carer of the above pupil, I confirm that I, with my child, have read and discussed Gorse Ride Schools Acceptable Use Agreement.

I understand that my son/daughter will have access to the internet and to IT systems at school. I am aware that this activity will be monitored for safety and security reasons to safeguard both my child and the schools' systems. This monitoring will take place in accordance with data protection and human rights legislation.

I know that my son/daughter has understood the Acceptable Use Agreement.

I know that my child has received, or will receive, online safety education to help them understand the importance of safe use of IT – both in and out of school.

I understand that the school will take every reasonable precaution, including filtering systems, to ensure that young people will be safe when they use the internet and IT systems. I also understand that although internet filtering systems usually work very well, inappropriate content may occasionally still be accessible, but in this instance the school will take appropriate action with the service provider to request such content is removed.

I fully support the school's online safety approaches and will encourage my child to adopt safe use of the internet and digital technologies at home.

I will inform the school if I have any concerns over my child's, or any other members of the school community's online safety.

I know that I can visit the following websites for further information about keeping my child safe online.

- www.thinkuknow.co.uk/parents
- www.internetmatters.org
- www.saferinternet.org.uk
- www.childnet.com

Parent/Carer's Name:	
Parent/Carer's Signature :	

ACCEPTABLE USE AGREEMENT - STAFF

This document is intended for all staff, temporary workers, volunteers and other parties who may have access to the schools' information systems.

Purpose

To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with pupils, they are asked to sign this code of conduct. Members of staff should consult the school's Online Safety policy for further information and clarification.

Declaration

- I understand that it is a criminal offence to use a school IT system for a purpose not permitted by its owner.
- I appreciate that IT includes a wide range of systems, including mobile phones, PDAs, digital cameras, e-mail, social networking and that IT use may also include personal IT devices when used for school business.
- I understand that school information systems may not be used for private purposes without specific permission from the Executive Head Teacher.
- I understand that my use of school information systems, internet and e-mail may be monitored and recorded to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager.
- I will not install any software or hardware (eg on a school laptop / device) unless authorised.
- I will ensure that personal data, particularly that of pupils, is stored securely through encryption and password and is used appropriately, whether in school, taken off the school premises or accessed remotely in accordance with the school Online Safety policy.
- I will respect copyright and intellectual property rights.
- I will ensure that electronic communications with pupils (including e-mail, instant messaging and social networking) and any comments on the web (including websites, blogs and social networking) are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
- I will promote online safety with pupils in my care and will help them to develop a responsible attitude to system use, communications and publishing.
- I will ensure that pupil use of the internet is consistent with the school's Online Safety Policy.
- When working with pupils, I will closely monitor and scrutinise what pupils are accessing on the internet including checking the history of pages when necessary.
- I will ensure that computer monitor screens are readily visible, to enable monitoring of what the children are accessing.
- I know what to do if offensive or inappropriate materials are found on screen or printer.
- I will report any incidents of concern regarding pupils' safety to the appropriate person, e.g. Online Safety Co-ordinator, Designated Safeguarding Lead and/or SLT member.

The school may exercise its right to monitor the use of the school's information systems, including internet access, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sounds.

Signed : _____

Print Name : _____

Position : _____

Date : _____