Garretts Green Nursery School & Enhanced Provision

Acceptable Use/ Internet Access Policy

At Garretts Green Nursery School & Enhanced Provision we respect and value all children and are committed to providing a caring, friendly and safe environment for all our pupils so they can learn, in a relaxed and secure atmosphere. We believe every pupil should be able to participate in all school activities in an enjoyable and safe environment and be protected from harm. This is the responsibility of every adult employed by, or invited to deliver services at, Garretts Green Nursery School. We recognise our responsibility to safeguard all who access school and promote the welfare of all our pupils by protecting them from physical, sexual and emotional abuse, neglect and bullying.

'Children have the right to XXXXXX.'

(United Nations Convention on the Rights of the Child, Article XXX).

Date of Review:

Signed:

Name/Position: Chair of Governors

Rationale

The use of ICT plays an increasingly important role in the lives of us all and is ever-changing and poses challenges to our understanding and safety.

This Acceptable Use Policy sets out the roles, responsibilities and procedures for the safe and appropriate use of all technologies and the use of the internet and provides guidelines for the safeguarding and use of ICT for all employees of Garretts Green Nursery School, both at school and also at home.

The policy recognises the ever-changing nature of emerging technologies and highlights the need for regular review to incorporate developments within ICT.

Scope of the policy

The policy applies to **all** employees of Garretts Green Nursery School, including any individuals working in a voluntary capacity or Governors supporting within school.
All schools are expected to ensure that non-employees on site are made aware of the expectations, so that technologies and the internet are used safely and appropriately.
The Acceptable Use Policy should be used in conjunction with the school disciplinary procedures and Code of Conduct applicable to employees.

Legal background

All adults who come into contact with children and young people in their work have a duty of care to safeguard and promote their welfare.

The legal obligations and safeguarding duties of all school employees in relation to use of technologies feature within the following legislative document which should be referred to for further information:
'Working Together to Safeguard Children Part1', September 2016

All safeguarding responsibilities of schools and individuals referred to within this Acceptable Use Policy includes, but is not restricted to, the legislation listed above.

Users must agree to comply with all software licence agreements and must not attempt to copy any software from, or by using school computers. If you have any requirements for using additional software for any reason, please seek advice from the Headteacher.

Technological devices in school

Devices provided for teachers use to plan, assess and resource teaching **may** be taken off-site. These appliances are likely to include:

- Teachers' Laptop
- Teachers' iPad
- USB memory sticks- encrypted
- Charges for devices – these must be available in school during school hours.

Devices are also provided for teachers' use but must be kept in school at all times and include:

- Curriculum/pupils' iPads
- School iPod
- School Mobile (not currently in use)
- School Cameras

A log of all ICT equipment issued to staff, including serial numbers, is maintained by the School Administrator.

Passwords **must be** used for all technological devices that are taken off-site (see password section). A record of these passwords will be retained confidentially in staff personnel files.

It is understood that in some cases staff complete school-related tasks off site, for example, it may be necessary to update assessments or SEN information outside school hours. Staff must ensure that personal/sensitive data and photography of children should only be saved/stored and transported on password protected devices in accordance with data protection expectations.

All staff, Governors and visitors understand that they are responsible for all activity carried out under their username.

Staff, Governors and visitors will not install any hardware or software on any school owned device without the Head Teacher's permission.

Smart Watches and Wearable Technology

Smart watches and other wearable technologies that can record images, audio, or access the internet are not permitted to be used during the school day unless explicit permission has been granted by a senior member of staff. These devices must be switched off or set to school mode and not used for communication, photography, recording, accessing applications, or the internet while on school premises. The use of smart watches must not compromise safeguarding, privacy, academic integrity, or data protection. Any misuse of wearable technology will be treated in line with the school's behaviour and safeguarding policies.

Mobile/Smart Phones

It is accepted that staff will have access to personal mobile phones which he/she will carry with them to school each day. However, staff are not permitted to use mobile phones in school during teaching time except in the main school office with agreement from the headteacher.

- Personal mobile phones are permitted on the school site, but should be used outside of lesson time only.
- Mobile phones must not be taken into the main Nursery block at any time during the day until the end of the afternoon when no children are present.
- Mobile phones may be used at lunch time in the main office or in the main staffroom- which is situated at the opposite end of the building to the classrooms. Once staff have finished their lunch breaks mobile phones must be stored back in their lockers.
- In exceptional circumstances, such as family illness, mobile phones may be left in the main office during teaching times. If an incoming call is heard this will not be answered but the member of staff concerned will be informed and he/she may return the call in the office only.
- All staff phones must be kept securely in staff lockers during school hours.
- It is the responsibility of the staff member to ensure that there is no illegal or inappropriate content stored on their device when brought onto school grounds.
- Personal mobile phones should not be used to contact parents.
- Personal mobile phones should never be used to contact children, young people or their families.
- Personal mobile phones should **never** be used to take photos of any children in the school.
- A school mobile should be taken on all school trips so as to contact staff and parents in the case of an emergency.
-

Teacher iPads/iPods

Teacher iPad use

The school provides teacher iPads which are believed to be essential to the learning and teaching of the pupils and the on-going assessment procedures using Tapestry. IPads should be used to enhance and record experiences.

- iPads should be kept safe and secure by the staff 'owner'.

- iPads can be taken off site by the owner (see managing remote access section)
- If taken off-site, iPads must be transported securely and must never be left on show in a car.
- iPads should have a passcode set up by the owner and should be passcode protected at all times.
- iPads can be used to record sensitive and secure information as they are password protected.
- iPads which are taken off-site are for the sole use of the member of staff and never for use by family members or friends.
- Staff should use iPads for school-related activities only, such as updating Tapestry

Teacher iPad Care, Security and Maintenance

I-Pads are expensive pieces of equipment which are costly to repair or replace and staff are expected to maintain high levels of care and maintain the safe physical use of the device.

- iPads must have protective covers/cases at all times.
- Users should be aware that the iPad screen is made of glass and should be used as carefully as possible.
- iPads must not be subjected to extreme temperatures.
- Teacher iPads should not be used by pupils unless supervised, (pupils should only use the teacher iPad to take pictures or videos).
- iPads should be returned to the Headteacher's office prior to staff leaving the building at the end of the day. They will then be locked securely in the Server Room over-night.
- iPads should be stored securely at the start and end of every session when the school is open to parents and carers.
- iPads must never be left on show during lunch breaks or before the start of teaching sessions.
- iPads should be locked in teachers' cupboards at these times.
- If the iPads are taken off site it is the responsibility of the staff member to keep them safe.
- School iPads must not be linked to personal iCloud accounts or other devices for personal use.
- iPads should be in school ready for the teachers use each day.
- Staff members are responsible for charging their iPads and for ensuring that chargers are maintained.
- Staff members are responsible for updating their iPads.
- Free iPad apps should be maintained through the staff personal apple account.
- Paid iPad apps should be purchased through the school apple account.

Curriculum iPads

Curriculum iPad use

Curriculum (children's) iPads should be used to enhance learning for pupils in teaching sessions only.

- Curriculum iPads should not be taken off-site.
- iPads must have protective covers/cases at all times.
- Adult supervision must be vigilant when children are using iPads
- Children must be encouraged to handle iPads carefully and wherever possible should be made aware that the iPad screen is made of glass.
- Pupils should be aware of the 'iPad rules poster' which is displayed in all classrooms and iPad use areas which lists the following rules;
    1. Hold the iPad with two hands.
    2. Always sit down when using the iPad.
    3. Turn the iPad screen off when the teacher is talking.
    4. Be gentle when tapping the iPad screen.
    5. Only use the app or website you have been asked to use.
    6. iPads must not be subjected to extremes in temperatures.

Curriculum iPad Care, Security and Maintenance

- iPads should be stored in a lockable unit overnight. They should never be left in classrooms.

- iPads should be unlocked at the start of the day by a designated member of staff (Emma Jarman)
- The designated member of staff should be the only key holder other than the HT or School Administrator
- iPads should be charged and ready to be used during teaching time.
- iPads should only be plugged into the charging unit at the end of the day if below 70% battery.
- iPad apps should be bought and maintained through the school Apple account.
- The whereabouts of all iPads should be known at all times by a designated member of staff, (e.g. iPads should be kept in the classroom of the class teacher who is using the iPads or in their charging unit).
- If any member of staff wish to use the iPads this should be recorded on the 'school iPad use' timetable.
- If an iPad is found unattended it should be given to the nearest member of staff.

School Laptops

School laptops are provided on loan to all teaching staff to enhance the learning and teaching experience, for example, for making resources, searching the internet for resources such as video material, etc.

As with iPads, laptops are expensive pieces of equipment which require care, secure use and maintenance. Staff are responsible for ensuring the best possible attention to the care, security and maintenance of the equipment provided.

- Staff must transport and use the laptop appropriately in accordance with makers guidelines (carried in a bag, used away from heat, etc)
- Carrying laptops off-site must be done securely with no laptop left on show in a car during transportation.
- Staff must sign in securely at least weekly, ensure that updates and synchronisation are enabled and then sign out appropriately.
- Staff must ensure that all sensitive school data is stored on the network (shared drive) and not solely on the laptop or device, unless the device is encrypted.
- In the event of loss or theft, failure to safeguard sensitive data could result in a serious security breach and subsequent disciplinary action.
- Password protection alone is not sufficient.
- Personal use of school laptops or computing facilities, whilst on site, is not permitted during teaching time but personal use outside school hours is allowed provided that the sites and materials accessed are secure and appropriate and do not breach the Code of Conduct.
- Staff are provided with laptops to allow for school related work to be completed off site.
- Personal use of the laptop from home (such as web browsing/online shopping etc) is permitted but should be kept to a minimum and use of the device is **strictly restricted** to the authorised member of staff only (i.e. **not** family members).
- Staff are aware that all activities carried out on school devices and systems, both within and outside of the school environment, will be monitored in accordance with this policy by Policy Central Forensic Maintenance.
- Staff will ensure that school laptops and devices are made available as necessary for antivirus updates, software installations, patches, upgrades or routine monitoring/servicing.
- Laptops must be available on alternate Thursdays (currently) when the school's ICT Technician is on-site.

Removable Media (Memory Sticks/USB)

- Where staff may require removable media to store or access sensitive data (e.g. IEPs, pupil attainment and assessment data) off site, encrypted memory sticks should be used.
- Any passwords used for encrypted memory sticks/or other devices will remain confidential to the user and shared only with the School Administrator and Headteacher for security and monitoring purposes.
- USB memory sticks must never be shared or used by other than the authorised user.
- USB memory sticks must be kept secure at all times both in school and off-site.

Managing Remote Access Use

As technology continues to develop at an exponential rate, schools and their staff are increasingly taking advantage of opportunities for off-site access to the school email and online assessment tool and off-site use of school technologies.

For data security and safeguarding purposes, it is crucial that staff are aware of the following restrictions on use:

- Only technological equipment with the appropriate level of security should be used off-site (e.g. password protected laptop and iPads).
- Usernames should be confidential to any non-staff members.
- Usernames should not use information that can be easily guessed (e.g. date of birth, telephone number, number patterns)
- Time out should be set on a school laptop to a minimum of 5 minutes.
- Access to Tapestry off-site must be confidential to school staff only and the site should be securely closed after use.
- VPN access has been enabled for senior staff. The school system may be accessed remotely as a result by restricted personnel only and care must be taken to ensure that access is disabled after use.

Passwords

Passwords should be selected carefully to ensure that they are effective in ensuring security of personal or sensitive data as well as limiting access to technology.

- Passwords should be used on any school technologies both in school and off site (School machines, Teacher iPad and Teacher Laptop) or any programs or internet sites which allow access to personal/sensitive information (Tapestry and email accounts) used on or off site.
- Passwords should be reset and changed as prompted.
- Passwords should not be shared with any other staff member or non-members of staff.
- Devices/technology should not be left unattended with open access (ie: staff must log off when leaving a machine and must not log in for others)
- Passwords are retained securely in staff personnel files for emergency access if required. Staff are expected to inform the Headteacher or School Administrator of any updates.

Email Use

Every member of staff has an email account which is accessed by secure password. Staff are able to access their school email account off-site.

- The school provides all staff with a professional email account to use for school related business.
- Communications with parents and carers via email is restricted to Senior Leaders whose professional role requires theses communications.
- Personal email accounts should never be used for school business to allow email content to be monitored and to protect staff from the risk of allegations, malicious emails or inappropriate contact with children and their families.
- Should parents or carers request contact through email, it is advisable to provide the main school enquiry address: enquiry@garretts.bham.sch.uk
- Staff may use their school email account to communicate with other staff employed by the school. However if staff make reference to a child, ensure that the child is only referred to by their initials.
- Many professional agencies provide secure access protocols and these should be followed strictly when communicating sensitive/confidential information.
- Under no circumstances will staff members engage in any personal communications (i.e. via Hotmail or Yahoo or other email accounts) with parents of current or former students.
- All emails should be professional in tone and checked carefully before sending, just as in the case of an official school letter.
- Staff should inform the Headteacher immediately if they receive an offensive or inappropriate email via the school system.

- It is the responsibility of each account holder to keep their password secure and to report any suspected breaches of password security to the Headteacher.
- Account holders must never share their password with another user, or allow access to their email account without the express permission of the Headteacher.
- Staff should avoid using the school email account for personal communications wherever possible.

Photography and Video Use

Digital photographs and videos are an important part of the learning experience for children and young people and, as such we have a responsibility to ensure that we not only educate pupils and their parents about the safe and appropriate use of digital imagery, but also model good practice ourselves. There are, therefore, strict protocols and procedures for staff about the use of digital imagery within school.

- Written consent will be obtained from parents or carers before photographs or videos of young people will be taken or used within the school environment, including for display within the building and for the school website or associated marketing material.
- Staff must use school devices, such as the school cameras or iPads to take photographs or videos of students. Staff must not use their personal mobile phones or cameras under any circumstances for taking photographs or videos of pupils or events.
- Where photographs of students are published or displayed (e.g. on the school website/blog) staff must ensure that they have checked children against the consent form (lists updated regularly and copies found in the school office)
- Where photographs of students are published on the school website/blog staff must ensure that no children are identified by name.
- Where photographs are used for displays in school, children should generally be identified by first names only.
- Photographs that are used as a form of assessment and are uploaded onto an assessment database (ie. Tapestry) may be accessed only by staff and/or the child's parents/carers who may access only their own child's information.
- No others should have access to Tapestry with the exception of the Headteacher, Assistant Headteacher and Administrator who are authorised to have an overview of the site.

Social Networking

The school currently uses facebook. It is understood that staff may use social networking sites in their own time beyond school. Where this is the case, staff must adhere to simple protocols to maintain their own safety and to protect the reputation of the school.

It is important to ensure that, in private, use of their own personal social networking site:

- Staff should maintain their professionalism while using social media sites (professionalism outlined in minimum standards).
- Staff must not include in their personal information any reference to their employment in the school.
- No reference should be made in social media to the school, pupils, pupils' parents/carers, students, governors or school staff, (either past or present).
- The nature of the posts on social media should be considered carefully before being made public in order to avoid unplanned reference to any of the above (eg: through backgrounds in photographs)
- Staff must not 'friend' any parent or student. It is understood that, as many of the school's staff live within the local community, this may be difficult as long-standing friendships may already be in place. In such cases, it is advised that staff break the social networking links for the time that the pupil is present in school. This is the only situation where a member of staff should have contact via social networking with a parent.
- They do not engage in online discussions on personal matters relating to members of the school community.
- Personal opinions should not be attributed to the school or LA.
- Security settings on personal social media profiles should be regularly checked to minimise the risk of loss of personal information.

Blogging

At Garretts Green Nursery School a blog is used as a link between home and school and is open to parents to access to comment on events and photographs.

- Photographs and videos of children can be uploaded onto the school blog by the website administration team (Lesley Martin, Claire Henebury and Emma Jarman) provided that there is strict adherence to the protocols for keeping children safe, as outlined above.
- Children's names are not used on the blog if presenting children's work.
- Any communication between home and school via the blog must be in an appropriate manner and always remain professional.
- Staff may comment on or add to the school's blog complying with protocols above.

Prohibited Use

Accessing inappropriate materials

All materials on the iPad must adhere to the ICT Acceptable Use Policy. Users are not allowed to send, access, upload, download or distribute offensive, threatening, pornographic, obscene or sexually explicit materials.

Illegal Activities

Use of the school's internet/email accounts for financial or commercial gain or for any illegal activity is not to be carried out.

Malicious Use and Vandalism

Any attempt to destroy hardware, software or data will be subject to disciplinary actions.

Jail breaking

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

Users should also be aware of and abide by the guidelines set out by the school's E - safety Policy.

In the event of staff misuse

If an employee is believed to have misused the internet or school network in an illegal, inappropriate or abusive manner, a report must be made to the Headteacher immediately.

The appropriate procedures for allegations must be followed and the following teams/authorities contacted:

- Schools' Senior HR Advisory Team
- School and Governor Support
- LADO (Local Authority Designated Officer)
- Police/CEOP (if appropriate)

In the event of minor or accidental misuse, internal investigations should be initiated and staff disciplinary procedures followed, only if appropriate.

Examples of inappropriate use

- Accepting or requesting pupils as 'friends' on social networking sites
- Exchanging personal email addresses or mobile phone numbers with parents or students.
- Behaving in a manner online which would lead any reasonable person to question an individual's suitability to work with children or act as a role model.

Garretts Green Nursery School

Staff Acceptable Use of Technologies Agreement

The core values of the Staff Acceptable Use Policy are safeguarding and responsible behaviours allowing children and the adults who surround them to safely enjoy all of the benefits that technology and the internet can offer.

The policy is also to ensure that all staff at Garretts Green Nursery School are confident in their use of technologies and the internet.

I have read and understood the above 'Staff Acceptable Use Policy' and agree to comply with the content of the Policy.

Signed:	**Date:**
Name (printed):	
Staff Role:	

I have read and understood the additional 'Internet Access Policy'.

I understand the safeguarding procedures and protocols in place to maintain online safety for pupils at Garretts Green Nursery School.
I am happy with the content of e-safety taught to pupils to ensure they are safe when using the internet.

Signed:	**Date:**
Name (printed):	
Staff Role:	

Garretts Green Nursery School and Children's Centre

Internet Access Policy Statement

Safeguarding Statement

At Garretts Green Nursery School we respect and value all children and are committed to providing a caring, friendly and safe environment for all our pupils so they can learn, in a relaxed and secure atmosphere. We believe every pupil should be able to participate in all school activities in an enjoyable and safe environment and be protected from harm. This is the responsibility of every adult employed by, or invited to deliver services at Garretts Green Nursery School. We recognise our responsibility to safeguard all who access school and promote the welfare of all our pupils by protecting them from physical, sexual and emotional abuse, neglect and bullying.

RATIONALE

Providing access to the internet in school contributes towards the raising of standards and supports the professional work of staff.

This policy outlines our purpose in providing e-mail facilities and access to the Internet at Garretts Green Nursery School and Children's Centre and explains how the school is seeking to avoid the potential problems that unrestricted internet access could give rise to.

INTERNET ACCESS IN SCHOOL

Staff and pupils have access to web sites worldwide offering educational resources, news and current events. There will be opportunities for discussion and exchange of information within the school community and others worldwide.

Staff have the opportunity to access educational materials and good curriculum practice, to communicate with the advisory and support services, professional associations and colleagues; exchange curriculum and administration data

with the Local Authority and Department for Education and Skills (DfES); receive up-to-date information and participate in government initiatives such as National Grid for Learning (NGfL).

The internet is also be used to enhance the school's management information and business administration systems.

Staff, including supply staff, will not be expected to take charge of an internet activity without training. Staff should be given opportunities to discuss the issues and develop good teaching strategies. All staff (including teachers, supply staff and teaching assistants) and any other adults involved in supervising children accessing the internet, will be provided with the School Internet Access Policy, and will have its importance explained to them.

Staff accessing social media sites must ensure that, as a result of their posts, the school is not brought into disrepute. The name of the school should not be used in blogs, social networking or any other context. Similarly, the name of the school, nor any comment which links the user to the school, should be used in social media site profiles or discussions.

Staff should not make links with parents (past or current) nor should they communicate with parents on social networking sites.

Photographs should be posted with care and only with the permission of others who may feature on the photographs.

Staff should never post photographs of children other than on the official school website.

Parents' attention will be drawn to the Policy which is available for parents and others to read on request and on the school website.

The use of the internet is monitored by Securus which is checked my DSL's weekly.

ENSURING INTERNET ACCESS IS APPROPRIATE AND SAFE

The internet is freely available to any person wishing to send e-mail or publish a web site and therefore some material available on the internet is unsuitable for children. The following key measures have been adopted to help ensure that our pupils are not exposed to unsuitable material:

- Our internet security is managed by the Local Authority, which provides a service designed for pupils including a "firewall" filtering system intended to prevent access to material inappropriate for children;
- Children using the internet will normally be working in the classroom, during lesson time and will be supervised by an adult (usually the class teacher) at all times;
- Staff will check that the sites pre-selected and vetted for pupil use and are appropriate to the age and maturity of pupils;
- Staff will be particularly vigilant when pupils are undertaking their own searches and will check that the children are following the agreed search plan;
- Pupils will not be taught to use e-mail in Nursery
- Our Rules for Responsible Internet Use will be posted near computer systems.
- The ICT co-ordinator will monitor the effectiveness of internet access strategies;
- The ICT co-ordinator will ensure that occasional checks are made on files to monitor compliance with the school's Internet Access Policy;
- The headteacher will ensure that the policy is implemented effectively;

- Methods to quantify and minimise the risk of pupils being exposed to inappropriate material will be reviewed in consultation with colleagues and advice from the Local Authority,

- Pupils will be taught to tell a teacher immediately if they encounter any material that makes them feel uncomfortable.

- It is unlikely that any inappropriate material will be seen by pupils in school due to the extent of security measures in place. Policy Central security would identify the nature, the computer and person logged on. In the unlikely event that there is an incident in which a pupil is exposed to offensive or upsetting material the school will wish to respond to the situation quickly and on a number of levels. Responsibility for handing incidents involving children will be taken by the ICT Co-ordinator and the DSL in consultation with the Head Teacher and the pupil's key worker. All the teaching staff will be made aware of the incident in Pupil Awareness at a Staff Meeting if appropriate.

- If one or more pupils discover (view) inappropriate material our first priority will be to give them appropriate support. The pupil's parents/carers will be informed and given an explanation of the course of action the school has taken. The school aims to work with parents/carers and pupils to resolve any issue;

- If staff or pupils discover unsuitable sites the ICT co-ordinator will be informed. The ICT co-ordinator will report the URL (address) and content to the Internet Service Provider and the Local Authority. If it is thought that the material is illegal, after consultation with the Local Authority, the site will be referred to the Internet Watch Foundation and the police.

- Pupils should be protected from any possibility of cyber-bullying through supported use of the internet in Nursery school

MAINTAINING SECURITY

We are aware that connection to the internet significantly increases the risk that a computer or a computer network may be infected by a virus or accessed by unauthorised persons.

The ICT co-ordinator and Technician will up-date virus protection regularly, will keep up-to-date with ICT news developments and work with the LEA and Internet Service Provider to ensure system security strategies to protect the integrity of the network are reviewed regularly and improved as and when necessary.

Staff must not use a USB device which has been used on a home computer without previously ensuring that a security scan has been run.

The school monitors computer use/ internet use, using Policy Central and retains reports for monitoring purposes.

USING THE INTERNET TO ENHANCE LEARNING

Pupils will learn how to use a web browser. Staff and pupils will begin to use the internet to find and evaluate information. Access to the internet will become a planned part of the curriculum that will enrich and extend learning activities and will be integrated into the class schemes of work.

As in other areas of their work, we recognise that pupils learn most effectively when they are given clear objectives for internet use.

Different ways of accessing information from the internet will be used depending upon the nature of the material being accessed and the age of the pupils:

- Access to the internet may be by teacher (or sometimes other-adult) demonstration;

- Pupils may access teacher-prepared materials, rather than the open internet;

- Pupils may be given a suitable web page or a single web site to access;
- Pupils accessing the internet will be supervised by an adult, normally their teacher, at all times.
- It is essential when a member of staff uses the internet to enhance learning that the search or site chosen has been checked beforehand for suitability. This is particularly important when accessing Youtube which can provide exciting materials for use with young children but which may also lead to pupils being exposed to inappropriate materials.

USING INFORMATION FROM THE INTERNET

In order to use information from the internet effectively, ICT is important for pupils to develop an understanding of the nature of the internet and the information available on ICT. In particular, they should know that most of the information on the internet is intended for an adult audience, much of the information on the internet is not properly audited/edited and most of ICT is copyright.

Staff will ensure that pupils are aware of the need to validate information whenever possible before accepting ICT as true, and understand that this is even more important when considering information from the internet (as a non-moderated medium).

Pupils will be made aware that the writer of an e-mail or the author of a web page may not be the person claimed.

USING EMAIL

ICT is important that communications with persons and organisations are properly managed to ensure appropriate educational use and that the good name of the school is maintained. Therefore:

- Staff will use email as part of their communications with a wide range of professionals, business contacts and others. This is monitored using Policy Central which captures inappropriate searches, comments, vocabulary and photographs. Staff will be challenged where concerns arise.
- Pupils will not be allowed to use email in Nursery
- Staff will endeavour to ensure that safety rules remain uppermost in their minds as they monitor children using the internet and should avoid the use of email with our pupils.
- The forwarding of chain letters will not be permitted.

THE SCHOOL WEBSITE

Our school website is intended to:

- Provide accurate, up-to-date information about our school;
- Enable pupils to publish work to a high standard, for a very wide audience including pupils, parents, staff, governors, members of the local community and others;
- Celebrate achievement;
- Promote the school.

All pupils may provide ‘work’ for publication on the school website. Staff will be responsible for ensuring that the content of the pupils' work is accurate and the quality of presentation is maintained. All material must be the child's own work but may not be attributed to the child by name. However, it is most likely that information included on the website will be in the form of photographs or videos, which will not identify any child by name nor include information about any child whose parents have not given prior consent.

The ICT co-ordinator, Emma Ashford, is responsible for up-loading information to the school website, ensuring that links work and are up-to-date, and that the site meets the requirements of the site host.

The point of contact on the website will be the school address, telephone number and e-mail address. We do not publish pupils' names alongside photographs that identify individuals on our web pages. Home information or individual e-mail identities will not be published. Staff will be identified by their first name only other than in the section regarding staffing information unless they request otherwise. Permission will be sought from other individuals before they are referred to by name on any pages we publish on our web site.

This does not apply, however, to school Governors whose details must be published on the school website following guidance from the DfE.

INTERNET ACCESS AND HOME/SCHOOL LINKS

Parents will be informed that pupils are provided with supervised internet access as part of their lessons. We will keep parents in touch with future ICT developments through the website, letters and newsletters.

School and Local Authority guidelines on issues such as safe internet use will be made available to parents together with printed information and internet sites providing information for parents about safe access for children.

RULES FOR RESPONSIBLE INTERNET USE

The school has installed computers with internet access to help our learning. These rules will help keep us safe and help us be fair to others. Pupils and Staff will:

- Only access the computer system with the login and password they have been given
- Always log off and close down the computer when leaving the computer unattended
- Not access files belonging to other staff members
- Report any unpleasant/inappropriate/offensive material immediately
- Understand that the school may check computer files and will monitor the internet sites visited
- Immediately report any inappropriate content
- Understand that e-mail messages received may be read by others.

This Policy should be read alongside the school's Acceptable Use Policy.