Galleywood Infant School

E-Safety Policy May 2014

Development, monitoring and review of the policy

This e-safety policy has been developed through a range of formal and informal meetings with:

- The Senior Leadership Team
- Subject leader for Computing
- Staff – including Teachers & Support Staff
- Safeguarding Governor, Learning and Ethos Committee, Full Governing Body
- Parents and Carers

Schedule for Development , Monitoring and Review

This e-safety policy was approved by the Full Governing Body	*July 2014*
The implementation of this e-safety policy will be monitored by the:	*Senior Leadership Team and the Governing Body*
Monitoring will take place at regular intervals:	*Annually, or more frequently if there is a concern.*
The Governors Learning and Ethos Sub Committee will receive a report on the implementation of the e-safety policy generated by the monitoring group (which will include anonymous details of e-safety incidents) at regular intervals:	*Annually, or more frequently if there is a concern.*
The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be:	*July 2015*
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	*Essex Safeguarding Children's Board, Essex Police, Schools Broadband Network*

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring of internet activity (including sites visited)
- Surveys / questionnaires from pupils, parents and staff.

Scope of the Policy

This policy applies to all members of the school community (including staff, pupils, volunteers, parents / carers, visitors) who have access to and are users of school IT systems, both in and out of the school.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

Roles and Responsibilities

Governors:

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Learning and Ethos Sub Committee receiving termly information about e-safety incidents and monitoring reports.

Safeguarding Governor (who also takes the role of E-Safety Governor) is responsible for:

- Regular informal meetings with the E-Safety Co-ordinator
- Regular monitoring of e-safety incident logs
- Questioning the E-Safety Co-ordinator about filtering / change control logs
- Holding the school to account for E-Safety responsibilities
- Taking part in staff training if appropriate

- Reporting to Governors' Learning and Ethos Committee
- Consulting parents both informally and as part of annual survey
- Liaising with the school and LA in the event of an incident

Headteacher and Senior Leaders:

- The Headteacher has a duty of care for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the E-Safety Co-ordinator.
- The Headteacher and Deputy Headteacher are aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. (see flow chart on dealing with e-safety incidents)
- The Senior Leaders are responsible for ensuring that the E-Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant. This is recorded in the CPD log.
- The Senior leaders will receive monitoring reports from the E-Safety Coordinator.
- The Headteacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. Where possible this will be undertaken by the E-Safety Coordinator and IT Technician together. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

E-Safety Coordinator :

- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provides training and advice for staff and maintains a log; signposts staff to relevant online information.
- liaises with the Local Authority, Essex Safeguarding Children Board and with technical staff.
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments.
- meets regularly with E-Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- reports regularly to Senior Leadership Team and once a year to Learning and Ethos Committee

School Computing Technician is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required e-safety technical requirements and the Essex E-Safety Policy
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are reviewed termly
- the filtering policy, is applied and updated on a regular basis, with codes recorded for reference
- that they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- that the use of the school network, Virtual Learning Environment , remote access and email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher for investigation and action.

Teaching and Support Staff are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- they have read, understood and signed the Staff Acceptable Use Agreement annually
- they report any suspected misuse or problem to the E-Safety Coordinator for investigation and action
- all digital communications with parents / carers should be on a professional level and only carried out using official school systems
- E-safety issues are embedded in all aspects of the curriculum, in our behaviour code and through assemblies
- pupils understand and follow our simple E-safety code

- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other relevant school activities and implement current policies with regard to these devices
- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Child Protection Designated Person

should be trained in E-safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

Pupils:

- should show that they understand and can work according to our 3 point Computing code.
- need to understand the importance of reporting anything they are uncomfortable with
- should understand the importance of adopting good e-safety practice when using digital technologies out of school

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through newsletters, letters, the school website and VLE and information about national / local e-safety campaigns. Parents and carers will be encouraged to support the school in promoting good e-safety practice and to follow guidelines on using:

- digital and video images taken at school events
- monitoring their children's use of the VLE and websites provided through the school
- access to parents' sections of the website

Policy Statements

Education - pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in e-safety is an essential part of the school's e-safety provision, helping and supporting children to recognise and avoid e-safety risks and build their resilience.

At Galleywood Infant School E-safety messages are reinforced across the curriculum in the following ways

- A planned e-safety curriculum is provided as part of Computing, PHSE and other lessons where relevant and should be regularly revisited
- Staff should act as good role models in their use of digital technologies the internet and mobile devices
- Internet use is pre-planned and pupils are guided to sites checked as suitable for their use; adults are working alongside children, who are reminded to notify us of any unsuitable material that is found in internet searches
- **Children are never allowed to freely search the internet**

Education – parents / carers and families

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities and information sessions including FS Coffee mornings
- Letters, newsletters, web site, VLE

- Promotion of high profile events such as Safer Internet Day
- Reference to the relevant web sites / publications including links to these from the school website
- Offering Family Learning courses in conjunction with Chelmsford College

Education & Training – Staff / Volunteers

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of e-safety training will be made available to staff. This will be regularly updated and reinforced. The IT subject leader will evaluate the response to training and identify any further/ new needs.
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Agreements.
- The E-Safety Coordinator will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- This E-Safety policy and its updates will be presented to and discussed by staff in staff meetings / INSET days.

Training – Governors

Governors should take part in e-safety training / awareness sessions by

- Attendance at training provided by the Local Authority Governors Association or led by local providers
- Participation in school training / information sessions for staff or parents

Technical – infrastructure / equipment, filtering and monitoring

It is the responsibility of the school to ensure that individuals providing technical support carry out all the e-safety measures suggested below and are fully aware of the E-Safety Policy and Acceptable Use Agreements.

Working with our technician the school is responsible for ensuring that the infrastructure / network is as safe and secure as is reasonably possible and that procedures approved within this policy are implemented. It will also ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

- School technical systems are managed in ways that ensure that the school meets recommended technical requirements outlined by Essex LA.
- There are regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling are securely located and physical access restricted
- All users have clearly defined access rights to school technical systems and devices.
- All users are provided with a username and password by Stacey Holden/ Steve Perry who will keep an up to date record. Users are responsible for the security of their username and password and will be required to change their password every year.
- The “administrator” passwords for the school IT system, used by the Network Manager must also be available to the Headteacher and kept in a secure place (e.g. school safe)
- Steve Perry 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
- **Internet access is filtered for all users.** Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. Any requests for filtering changes need to be made to the E-Safety Coordinator and may be auctioned by Steve Perry via the Essex Broadband service.
- The school has provided differentiated user-level filtering. Staff should be aware of the risks of using their adult logon with children- see appendix.
- Any actual / potential technical incident / security breach must be reported immediately to the E-safety coordinator, to the Headteacher and Finance Officer.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- Temporary “guest” login access can be provided (e.g. for trainee teachers, supply teachers, visitors, volunteers) onto the school systems- contact IT Subject leader, Steve Perry. These will be recorded and use may be monitored. Temporary logins do not have access to photos.

- Staff are reminded at least annually that when using laptops out of school they should close any files that relate to Galleywood Infant School and securely log out.
- Photos and personal data should be stored securely on the main server and not on laptops. Memory sticks may be used to transfer photos or personal data but should not be used to store files and should not be removed from school. See School Personal Data Policy- appendix.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyber bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- **When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images, in particular the risks attached to publishing their own images on the internet e.g. on social networking sites.**
- **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 (as such use is not covered by the Data Protection Act). 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 students / pupils in the digital / video images.**
- **Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.**
- **Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.**
- **Pupils must not take, use, share, publish or distribute images of others without their permission**
- **Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.**
- **Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.**
- **Written permission from parents or carers will be obtained before photographs of students / pupils are published on the school website. This will be part of the Acceptable User Agreement requested on admission**

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

(See School Personal Data template- appendix)

The school must ensure that:

- It 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".

- It has a Data Protection Policy (template in appendix- Sch has Data Protection Policy in place)
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
- Responsible persons are appointed / identified - Senior Information Risk Officer (SIRO) and Information Asset Owners (IAOs)
- Risk assessments are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from information risk incidents
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties

Staff must ensure that they:

- **At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.**
- **Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.**
- **Transfer data using encryption and secure password protected devices.**

When personal data is stored on any portable computer system:

- the data must be encrypted and password protected
- the device must be password protected
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and parents / carers (email, chat, VLE etc) must be professional in tone and content. Personal email addresses, text messaging or social media must not be used for these communications except in exceptional circumstances with the consent of the Senior Leadership team.
- Whole class / group email addresses may be used at KS1.

Social Media - Protecting Professional Identity

With an increase in use of all types of social media for professional and personal purposes this policy sets out clear and essential guidance for staff to manage risk and behaviour online. We promote as a core message the protection of pupils, the school and the individual when publishing any material online. Expectations for teachers' professional conduct are set out in 'Teachers Standards 2012'. Ofsted's e-safety framework 2012, reviews how a school protects and educates staff and pupils in their use of technology, including what measures would be expected to be in place to intervene and support should a particular issue arise.

All schools, academies and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools/academies and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyber bully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:

- Training to include: acceptable use, social media risks, checking of settings, data protection, reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School staff should ensure that:

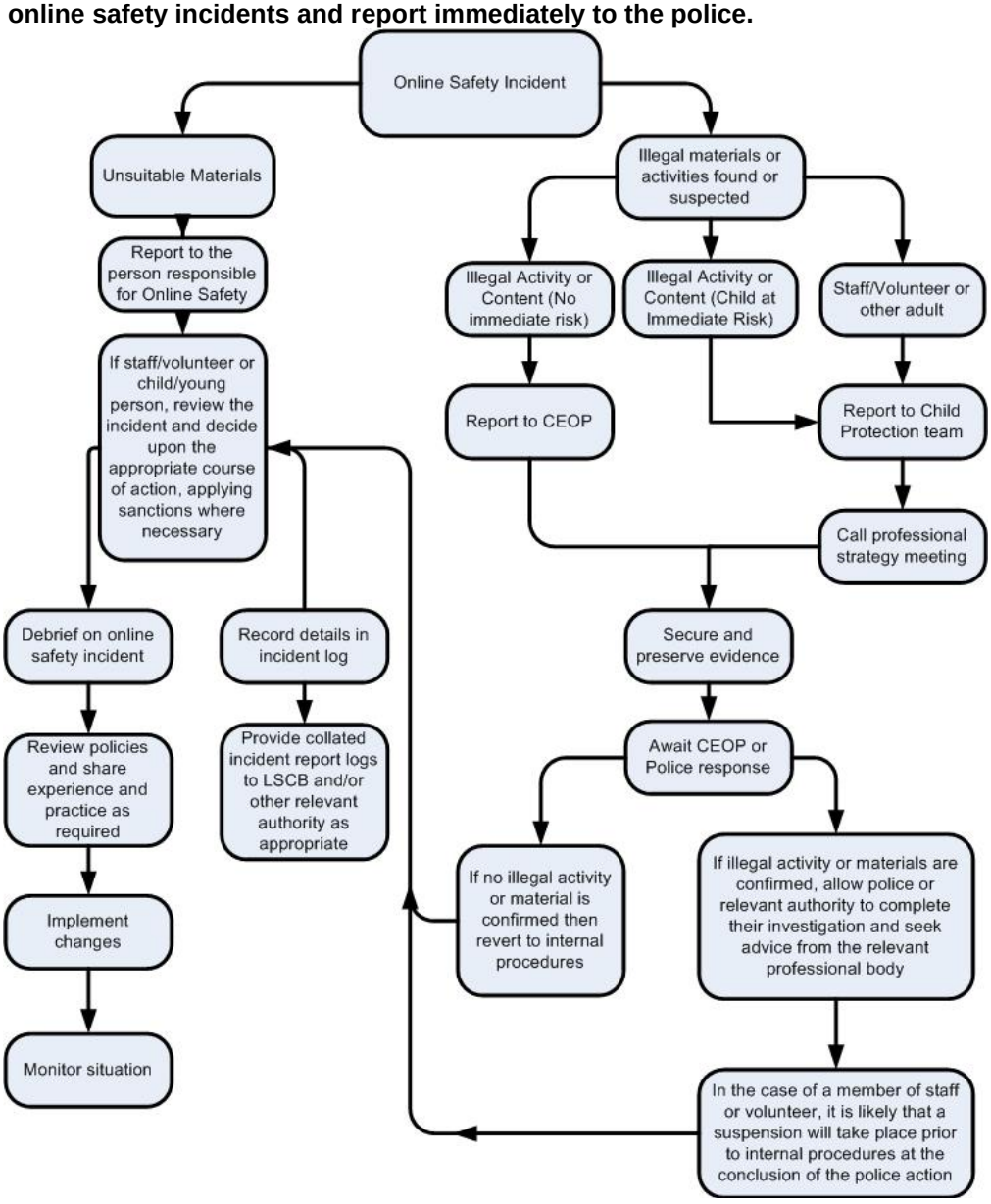
- No reference should be made in social media to students / pupils, parents / carers or school staff

- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to Galleywood Infant School or Essex local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see "User Actions" above).

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.



Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.

- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
  - Internal response or discipline procedures
  - Involvement by Local Authority or national / local organisation (as relevant).
  - Police involvement and/or action
- **If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:**
  - incidents of 'grooming' behaviour
  - the sending of obscene materials to a child
  - adult material which potentially breaches the Obscene Publications Act
  - criminally racist material
  - other criminal conduct, activity or materials
- **Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.**

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

School Actions & Sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures.

Appendix 1
Acceptable Use Agreement

Galleywood Infant School

Parent / Carer Acceptable Use Agreement: Computing

Digital technologies have become integral to the lives of children and young people, 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. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that young people 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 young people with regard to their on-line behaviour.

The school will ensure that pupils have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users. A copy of the Pupil Acceptable Use Policy is attached to this permission form, so that parents / carers will be aware of the school expectations of the young people in their care. It is displayed prominently in every classroom.

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

Permission Form

Parent / Carers Name | Pupil Name

As the parent / carer of the above pupil, 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 in ways appropriate for their age and level of understanding. 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 young people 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.

Signed | Date

Galleywood Infant School
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 lessons and in classroom displays.

Images may also be used to celebrate success through their publication in newsletters, the school prospectus, on the school website and Parents' Association website, and occasionally in the public media.

The school will comply with the Data Protection Act and request parents / carers permission before taking images of members of the school. We will also ensure that when images are published the young people **cannot** be identified by the use of their names.
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 (as such use is not covered by the Data Protection Act). 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.

Parents / carers are requested to sign the permission form below to allow the school to take and use images of their children and for the parents / carers to agree to the guidelines relating to images taken for home use.

Digital / Video Images Permission Form

Parent / Carers Name

Student / 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. Names never accompany photographs.

Yes / No

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.

Yes / No

Signed

Date

Galleywood Infant School

Pupil Acceptable Use Policy Agreement

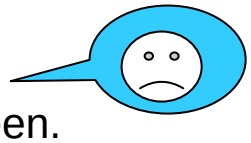
This is how we stay safe when we use technology:

I will **ask** an adult if I want to use the computers or iPads

I will **only use** activities that the adult has told or allowed me to use.

I will **take care** of the computer and other equipment

I will **ask for help** from an adult if I am not sure what to do or if I think I have done something wrong.



I will **tell an 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 or an iPad.

Signed (child):……

Signed (parent): ……..