Hoylandswaine Primary School

E-Safeguarding Policy
April 2019

Introduction

The internet is an essential element in 21st century life for education, business and social interaction and the school has a duty to provide children and young people with quality access as part of their learning experience. It is the duty of the school to ensure that every child and young person in its care is safe. E-Safeguarding encompasses internet technologies and electronic communications such as mobile phones and wireless technology. The purpose of internet use in school is to help raise educational standards and promote pupil achievement. This policy highlights the internet use to educate children and young people about the benefits and risks of using new technology and provide safeguards and awareness for users to enable them to control their online experiences.

This policy has been developed to ensure that all stakeholders and working together to safeguard and promote the welfare of children. E-Safeguarding is a safeguarding issue not an ICT issue and all members of the school community have a duty to be aware of E-Safeguarding at all times, to know the required procedures and to act on them. Safeguarding and promoting the welfare of pupils is embedded into the culture of the school and its everyday practice and procedures. All staff have a responsibility to support E-Safeguarding practices in school. Concerns related to child protection will be dealt with in accordance with the school's Safeguarding Policy and should be reported to the designated persons.

The policy is to be referenced alongside the safer use of the internet, data protection, social media, safeguarding, behaviour and anti-bullying policies.

Roles & Responsibilities

The Governing Body of the school will ensure:

- There is a senior member of the school's leadership team who is designated to take the lead on E-Learning/Safety within the school (Mr D Bond)
- There is a robust system for incident reporting. Procedures are in place for dealing with breaches of E-Safety and security and are in line with Local Authority procedures (e-safety written log and electronic log)
- All staff and volunteers have access to appropriate ICT training.
- They have read, understand and contribute to and help promote the school's E-Safeguarding policies and guidance.
- Appropriate funding and resources are available for the school to implement their E-Safeguarding strategy.

The Senior Leadership Team will ensure:

- All staff are included in E-Safeguarding training. Staff must also understand that misuse of the internet may lead to disciplinary action and possible dismissal.
- A Designated Senior Member of Staff for E-Learning/Safety is identified and receives appropriate on-going training, support and supervision and works closely with the Designated Person for Safeguarding.
- All temporary staff and volunteers including students are made aware of the school's E-Safeguarding Policy and arrangements.
- A commitment to E-Safeguarding is an integral part of the safer recruitment and selection process of staff and volunteers.
- Mr D Bond is designated as the Senior Information Risk Officer (SIRO) to assess the risk of the use of different types of technology and information data sets that are owned by the school.
- Develop and promote an E-Safeguarding culture within the school community.
- Support the E-Safeguarding Leader in their work.

The Designated Senior Member of Staff for E-Safeguarding (Mr D Bond) will ensure:

- Act as the first point of contact with regards to breaches in e-safety and security.
- Liaise with the Designated Person for Safeguarding as appropriate.
- Ensure that ICT security is maintained.
- Attend appropriate training.
- Provide support and training for staff, governors and volunteers on E-Safeguarding.

- All staff, governors and visitors read and sign the schools acceptable use agreement.
- All staff and volunteers understand and aware of the school's E-Safeguarding policy.
- Ensure that the school's ICT systems are regularly reviewed with regard to security.
- Ensure that the virus protection is regularly reviewed and updated.
- Discuss security strategies with the LA particularly where a wide area network is planned.
- E-Safeguarding education is embedded across the curriculum.
- E-Safeguarding is promoted to parents and carers.
- The Senior Information Risk Officer (SIRO) has carried out appropriate risk assessments dealing with the use of ICT equipment and technologies and the information data sets owned by the school.
- An E-Safeguarding incident log is kept up-to-date and regularly monitored/reviewed termly by the incident management team (E-Safeguarding coordinator, SIRO if different from the E-Safeguarding coordinator, ICT technician and where possible a designated member of the governing body).

The ICT Technician and SLA provider (Code Green) will ensure:

- The school's ICT infrastructure is secure and is not open to misuse or malicious attack.
- The school meets the E-safeguarding technical requirements outlined in the LA Security Policy and Acceptable Usage Policy and any relevant Local Authority E-Safeguarding Policy and guidance.
- Users may only access the school's networks through a properly enforced password protection policy.
- Code Green is informed of issues relating to the filtering applied.
- The school's filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.
- They keep up to date with E-Safeguarding technical information in order to effectively carry out their E-Safeguarding role and to inform and update others as relevant.
- The use of the network and e-mail is regularly monitored in order that any misuse or attempted misuse can be reported to the E-Safeguarding coordinator for investigation.
- Monitoring software and systems are implemented and updated as agreed in school policies.

Teachers and Support Staff will:

- Read, understand and help promote the school's E-Safeguarding policies and guidance.
- Read, understand and adhere to the school staff Acceptable use Policy (AUP).
- Develop and maintain an awareness of current E-Safeguarding issues and guidance.
- Model safe and responsible behaviours in their own use of technology.
- Embed E-Safeguarding messages in learning activities where appropriate.
- Supervise children carefully when engaged in learning activities involving technology.
- In lessons where internet use is pre-planned children 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 on internet searches.
- Are aware of E-Safeguarding issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices.
- Be aware of what to do if an E-Safeguarding incident occurs by informing the E-Safeguarding coordinator or a member of the Senior Leadership Team.
- Maintain a professional level of conduct in their personal use of technology at all times.

The Child Protection Co-ordinator:

Mrs L Cole and Mr D Bond are trained in E-Safeguarding issues and are aware of the potential for serious child protection issues to arise from:

- Sharing of personal data
- Access to illegal/inappropriate materials
- Inappropriate online contact with adults/strangers
- Potential or actual incidents of grooming
- Cyberbullying

Children will:

- Be responsible for using the school ICT systems in accordance with the Acceptable Use Policy, (which parents/carers sign on behalf of the children before being given access to school systems) and the E-Safeguarding charter created by children on a yearly basis.
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking/use of images and on cyberbullying.
- Understand the importance of adopting good E-Safeguarding practice when using digital technologies out of school and realise that the school's E-Safeguarding policy covers their actions out of school, if related to their membership of the 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. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through parents' seminars, newsletters, letters, website and information about national/local E-Safety campaigns/literature. Parents and carers will be responsible for:

- Endorsing (by signature) the Pupil Acceptable Use Policy.

Teaching & Learning

Education – Children

E-Safety education will be provided in the following ways:

- In accordance with the 2014 National Curriculum requirements, planned e-safety teaching will be provided as part of Computing/PSHE/other curriculum areas (as relevant) and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school.
- Key e-safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities.
- Children should be taught in all lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of information.
- Children should be helped to understand the need for the pupil AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside of school.
- Children should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Rules for use of school computers/laptops/iPads/internet will be devised annually through discussion with children. These will be displayed in classrooms.
- Staff should act as good role models in their use of ICT, the internet and mobile devices.

Education – Parents/Carers

Although, it is recognised many parents and carers have only a limited understanding of e-safety risks and issues, they undoubtedly play an essential role in the education of their children and in the monitoring/regulation of the children's online experiences.

With this in mind, the school will therefore seek to provide information and awareness to parents and carers through:

- Letters and newsletters
- Parent workshops
- Reference to relevant online guidance provided by the school website or in paper format

Education & Training – Staff

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:

- Formal e-safety training will be made available to staff as appropriate.
- All new staff receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable use Policy.
- The E-Safeguarding Leader will receive regular updates through attendance of LA courses, other information sources and training sessions and by reviewing guidance documents released by BECTA. They are now a CEOP Ambassador.
- This E-Safety policy and its updates will be presented to and discussed by staff in staff meetings.
- The E-Safety Coordinator will provide advice, guidance and training to individuals as required.

Training – Governors

Governors should take part in e-safety training/awareness sessions, with particular importance for those who are members of any subcommittee, group involved with ICT, e-safety, health and safety and child protection.

This may be offered in a number of ways:

- Attendance at training provided by the Local Authority, National Governors Association or other relevant organisations.
- Participation in school training and information sessions for staff or parents.

The Curriculum

E-Safety should be a continuing focus in all areas of the curriculum and staff should reinforce E-Safety messages, wherever possible, in the use of computing across the curriculum.

- Where internet use is pre-planned, children should be guided to sites checked as suitable for their use by making use of shortcuts and bookmarks. Processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where children are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the children visit, this encouraging responsible use.
- It is accepted that from time to time, for good educational reasons, children may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the ICT Technician can temporarily remove those sites from the filtered list for the period of study. Any request should initially be brought to the E-Safeguarding Leader (Mr D Bond) with clear reasons provided.
- Children should be taught in all lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of information.
- Children should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

Managing Information Systems

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

- There will be regular reviews and audits of the safety and security of school ICT systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to school ICT systems.
- All users will be provided with a username and password by the ICT Technician who will keep an up to date record of users and their usernames.
- The "administrator" passwords for the school ICT system, used by the ICT Technician must also be available to the E-Safeguarding Leader and kept in a secure place.
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- The school maintains and supports the managed filtering service provided by Code Green.
- In the event of the ICT Technician needing to switch off the filtering for any reason, or for any user, this must be carried out by a process that is agreed by the E-Safeguarding Leader.
- Any filtering issues should be reported immediately to the E-Safeguarding Leader.

- Requests from staff for sites to be removed from the filtered list will be considered by the ICT Technician and E-Safeguarding Leader.
- The ICT Technician and E-Safeguarding Leader regularly monitor and record the activity of children on the school ICT systems and users are made aware of this in the Acceptable use Policy.
- An appropriate system is in place for users to report any actual/potential e-safety incident to the E-Safeguarding Leader or ICT Technician. The issue would be reported in the log and dealt with accordingly.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices, etc. from accidental or malicious attempts which might threaten the security of the school systems and data.
- An agreed policy is in place for the provision of temporary access of guests (e.g. students, visitors) onto the school system using general logins.
- An agreed policy is in place regarding the extent of personal use that users (staff/children/community users) and their family members are allowed on laptops and other portable devices that may be used out of school.
- An agreed policy is in place that allows staff to/forbids staff from installing programs on school workstations/portable devices.
- An agreed policy is in place regarding the use of removable media (e.g. memory sticks/CDs/DVDs) by users on school workstations/portable devices.
- The school infrastructure and individual workstations are protected by up to date virus software.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Managing Passwords

Passwords are an important part of computer security; they are a form of authenticating a user against a given username.

- All staff are to have passwords with consideration given to minimum password length and complexity, utilising both upper and lowercase letters, numbers and special characters.
- All children will have passwords that contain at least one uppercase letter and a number.
- Passwords will be changed every 90 days under the direction and with discretion of the ICT Leader.

Communication Technologies

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

- The official school e-mail service may be regarded as safe and secure and is monitored.
- Users need to be aware that e-mail communications may be monitored.
- Users must immediately report, to the Headteacher or E-Safeguarding Leader – in accordance with the school policy, the receipt of any e-mail that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such e-mail.
- Any digital communication between staff and children, students, parents/carers must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal e-mail addresses, text messaging or public chat/social networking programs must not be used for these communications.
- Children are not allowed personal e-mail addresses in school.
- Whole-class or group e-mail addresses will be used for communication with others.
- Incoming e-mail should be monitored by the class teacher and attachments should not be opened unless the author is known.
- Students and children should be taught about e-mail safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate e-mails and be reminded of the need to write e-mails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the school website and only official e-mail addresses should be used to identify members of staff.

Managing School Website Content

- Editorial guidance will ensure that the school's ethos is reflected in the website, information is accurate, well presented and personal security is not compromised. Care will be taken to ensure that all information is considered from a security viewpoint including the use of photographic material.
- Photographs of children will not be used without the written consent of the pupil's parents/carers.
- The point of contact on the school website will be the school address, school e-mail and telephone number. Staff or children's home information will not be published.
- The ICT Leader will have overall editorial responsibility and ensure that all content is accurate and appropriate.
- The website will comply with the school's guidelines for publications and parents/carers will be informed of the school's policy on image taking and publishing.
- Use of site photographs will be carefully selected so that pupils cannot be identified or their image misused. The full names of children will not be used on the website, particularly in association with any photographs. First names or initials will be displayed.
- Work will only be used on the website with the permission of the pupil and their parents/carers.
- The copyright of all materials must be held by the school or be attributed to the owner where permission to reproduce has been obtained.

Filtering

- The school will work in partnership with parents/carers; the Local Authority, the DFE and the Internet Service Provider (Code Green) to ensure systems to protect pupils and staff are reviewed and improved regularly.
- **ALL** internet usage will be monitored for inappropriate use.
- If staff or children discover unsuitable sites, the URL (address) and content must be reported to the E-Safeguarding Leader.
- Any material the school deems to be unsuitable or illegal will be immediately referred to the Internet Watch Foundation (www.iwf.org.uk) and the local authority.
- Regular checks by the ICT Technician and E-Safeguarding Leader will ensure that the filtering methods selected are appropriate, effective and reasonable.
- The level of filtering and content available will be selected by the school in conjunction with the LA and will be age and curriculum appropriate.

Dealing with Unsuitable/Inappropriate Activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in / or outside the school when using school equipment or systems. The school policy restricts usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	Pornography				X	
	Promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	Promotion of extremism or terrorism				X	
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					X	
On-line gaming (educational)			X			
On-line gaming (non-educational)					X	

On-line gambling				X	
On-line shopping / commerce				X	
File sharing				X	
Use of social media				X	
Use of messaging apps				X	
Use of video broadcasting e.g. Youtube – Staff only			X		

Use of Mobile Devices

- Children are not permitted to bring into school mobile devices such as mobile phones and handheld games. Staff have the right to confiscate these.
- Staff are allowed to bring mobile phones onto the school premises. These have to be stored with personal belongings out of reach of children. Staff under no circumstances should be using their mobile phones during lesson times especially when working with children. Staff are not permitted to take photographs of children on their mobile phones for security reasons.
- Staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity.
- Sexting – Children in Year 5 and 6 will be informed about the implications of sexting and how, once a picture has been sent, this image can never fully be removed from the World Wide Web.

Use of Digital and Video Images

When using images and video, staff and children need to be aware of the risks associated with sharing images and with posting digital images on the internet. It is vital both staff and children are aware of and take responsibility for their digital footprint. Images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying 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 children about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing their own images on the internet, e.g. on social networking sites.
- Staff 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, under no circumstances should the personal equipment of staff be used for such purposes.
- Photographs published on the website, or elsewhere that include children will be selected carefully and comply with parental choice on the use of images.
- Children's full names will not be used anywhere on a website or blog, particularly in association with photographs. First names or initials will be displayed.
- Written permission from parents or carers will be obtained before photographs of children are published on the school website. An updated list will be kept by the E-Safeguarding Leader and the school office. This list will also be given to all staff.

Protecting Personal Data

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.

The school must ensure that:

- It has a Data Protection Policy.
- It has paid the appropriate fee to the Information Commissioner's Office (ICO).
- It has appointed a Data Protection Officer (DPO).

- 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.
- Data held must be accurate and up to date. Inaccuracies are corrected without unnecessary delay.
- The lawful basis for processing personal data (including, where relevant, consent) has been identified and documented and details provided in a Privacy Notice.
- Where special category data is processed, a lawful basis and a separate condition for processing have been identified.
- Data Protection Impact Assessments (DPIA) are carried out.
- It has clear and understood arrangements for access to and the security, storage and transfer of personal data, including, where necessary, adequate contractual clauses or safeguards where personal data is passed to third parties e.g. cloud service providers.
- Procedures must be in place to deal with the individual rights of the data subject i.e. a Subject Access Requests to see all or a part of their personal data held by the data controller.
- There are clear and understood data retention policies and routines for the deletion and disposal of data.
- There is a policy for reporting, logging, managing and recovering from an information risk incident which recognises the requirement to report relevant data breaches to the ICO within 72 hours of the breach, where feasible.
- Consideration has been given to the protection of personal data when accessed using any remote access solutions.
- All schools must have a Freedom of Information Policy which sets out how it will deal with FOI requests.
- All staff receive data handling awareness / data protection training and are made aware of their responsibilities.

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, including the use of Forticlient.

When personal data is stored on any portable computer system, memory stick or any other removable media:

- 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 once it has been transferred or its use is complete.

Social Networking, Social Media and Personal Publishing

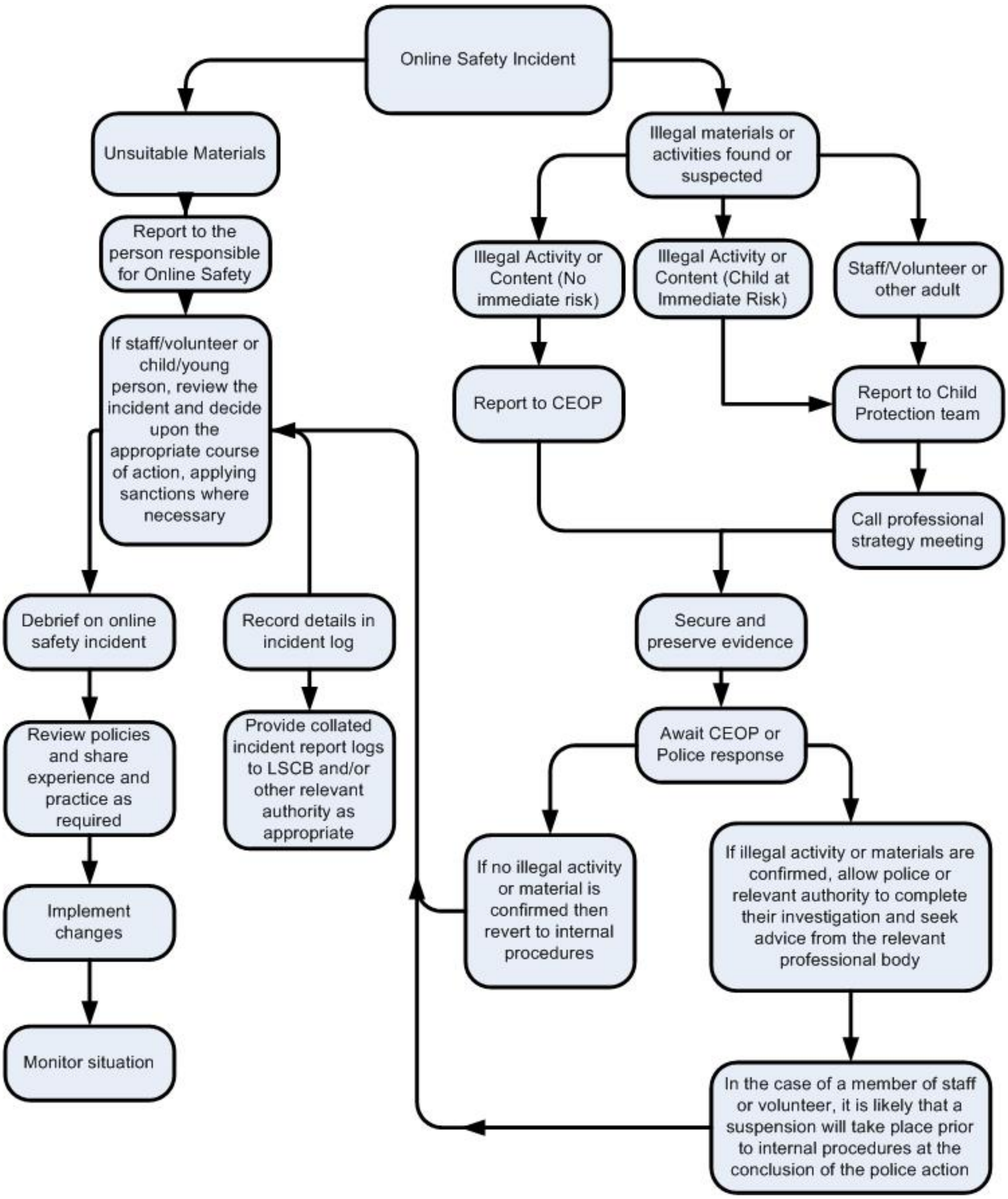
- Staff using social media websites such as Facebook and Twitter will not bring the school or their own professional status into disrepute.
- Guidance on security settings for Facebook and other sites is available from the E-Safeguarding Leader and instructions should be followed in line with the schools Social Media Policy.
- Staff should be aware that it is prohibited to add children as friends.
- Staff will not discuss professional matters on social media sites.
- Through the work of 'Thinkuknow' staff will teach children the importance of protecting data.

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.

Illegal Incidents

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 for responding to online safety incidents and report immediately to the police.


Online Safety Incident
Unsuitable Materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Review policies and share experience and practice as required
Implement changes
Monitor situation
Record details in incident log
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Illegal materials or activities found or suspected
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Secure and preserve evidence
Await CEOP or Police response
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action

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 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
    - 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
- promotion of terrorism or extremism
- 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 safeguarding 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 as follows:

	Actions / Sanctions								
Students / Pupils Incidents	Refer to class teacher	Refer to E-Safeguarding Lead	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security etc.	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction e.g. exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X					
Unauthorised use of non-educational sites during lessons		X				X			
Unauthorised / inappropriate use of mobile phone / digital camera / other mobile device	X					X		X	
Unauthorised / inappropriate use of social media / messaging apps / personal email		X				X			
Unauthorised downloading or uploading of files		X				X			
Allowing others to access school network by sharing username and passwords		X					X		
Attempting to access or accessing the school network, using another pupil's account		X					X		
Attempting to access or accessing the school network, using the account of a member of staff		X				X	X		
Corrupting or destroying the data of other users		X				X	X		
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X	X				X		
Continued infringements of the above, following previous warnings or sanctions		X	X				X		
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X	X				X		
Using proxy sites or other means to subvert the school's filtering system		X					X		
Accidentally accessing offensive or pornographic material and failing to report the incident		X				X			
Deliberately accessing or trying to access		X	X			X	X		

offensive or pornographic material									
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act		X							

	Actions / Sanctions							
Staff Incidents	Refer to E-Safeguarding Lead	Refer to Headteacher	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X				
Inappropriate personal use of the internet / social media / personal email		X						
Unauthorised downloading or uploading of files	X							
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	X					X		
Careless use of personal data e.g. holding or transferring data in an insecure manner	X					X		
Deliberate actions to breach data protection or network security rules	X	X				X		
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X	X				X		
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X				X		
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	X	X	X					X
Actions which could compromise the staff member's professional standing		X	X					X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X	X				X		

Using proxy sites or other means to subvert the school's filtering system	X					X		
Accidentally accessing offensive or pornographic material and failing to report the incident	X							
Deliberately accessing or trying to access offensive or pornographic material	X	X				X		
Breaching copyright or licensing regulations	X	X				X		
Continued infringements of the above, following previous warnings or sanctions	X	X	X					X

Dealing with Complaints

- Staff, children and parents/carers must know to report incidents to the Headteacher. Concerns related to Safeguarding issues must be dealt with through the school's Safeguarding Policy and Procedures.
- Complaints about internet misuse will be dealt with under the School's complaints procedure.
- All e-safety complaints and incidents will be recorded by the school, including any actions taken.
- The school's designated person for E-Safeguarding (Mr D Bond) will be responsible for dealing with complaints and any complaint concerning staff or child misuse of the internet must be reported to the Headteacher immediately. Any misuse will be recorded electronically.
- Parents/carers and children will work in partnership with the school staff to resolve any issues.
- Sanctions for misuse for pupils may include any or all of the following:
    - Discussions with the Headteacher
    - Informing parents/carers
    - Removal of internet access for a specified period of time

Through all these measures we hope that children have a positive experience when using the Internet and that ICT can be used as a tool to further develop and teach vital life skills allowing children to make a positive contribution.

Inclusion

The policy will be applied to all children. We welcome our general responsibilities under the Disability Equality Duty by promoting equal opportunities, eliminating discrimination and improving access to learning for disabled people. In order to comply with the requirements of the Equality Act 2010 we will make reasonable adjustments to ensure all stakeholders understand and can follow this policy. We will actively seek to remove any barriers to learning and participation that may hinder or exclude individuals or groups of children.

Acceptable use Policy

Use of the internet is now an integral part of people's lives. In spite of this, it is important schools continue to be aware of issues and problems and to continue to educate our children accordingly. It is important staff, children and parents understand the moral and ethical issues surrounding access to the internet before allowing access.

There are a number of options available that restrict access to the internet, but it must be understood that no system, other than a ban on using the internet, can ensure users do not access material that is deemed inappropriate. Pornographic material is usually the main focus of filtering methods, but users need to be aware that removing racist, sexist and political material is beyond many filtering programs. There is also the difficulty with any filtering software that content which is deemed offensive to one group of people is regarded differently by others. Furthermore, we are now faced with more recent issues such as grooming, cyberbullying and identity theft which cannot be controlled by filtering systems. For these reasons, treating the use of the internet as an issue that involves children, staff and parents has to be the most sensible approach.

In response to this, the most appropriate course of action is to develop a school policy on use of the internet together with a home/school agreement.

Hoylandswaine Primary School has an Acceptable Use Policy, together with rules for safe internet use. These rules are a joint agreement between staff and children as part of our E-Safety curriculum. The policy is available to parents on request and electronically via our website.

Today millions of people use the internet and e-mail on a daily basis. In recent years, use of the internet has continued to increase, particularly with the introduction of mobile devices. This is not only for business and personal use, but also for educational purposes. A wealth of educational resources is now available on the internet and via mobile devices; and this continues to grow. At Hoylandswaine Primary School, we believe that our pupils should have opportunity to use these emerging and changing technologies to support their learning and to equip themselves with the skills that will be required for lifelong learning.

Resources found on the internet, are unlike those found in more traditional media. Historically, resources such as books, videos and other resources could be carefully selected for the learning process. The internet, by its open and dynamic nature, may lead pupils to material over which the teacher has had no previous viewing and has therefore been unable to judge its suitability for classroom use. Although the school will endeavour to point children to relevant curriculum sites or to previously researched sites that have been identified as being relevant to the area of study, we also accept our responsibility in educating our children about responsible, respectful and safe use of the internet.

Research using electronic methods is now fundamental to preparing children for citizenship and future employment possibilities. The school will ensure that opportunities for both integrating the use of the internet into the curriculum and teaching children about e-safety will be planned and that staff will guide children in line with Government guidelines.

The school recognises that training the staff in preparation for using the internet and indeed any mobile technology in a safe manner is vital. The school will use a variety of agencies to train the staff in integrating new technologies into the curriculum. Staff will be given regular opportunities to discuss issues surrounding the use of the internet and e-safety and develop appropriate teaching strategies. In addition, relevant governmental guidelines will be made available to all staff as a point of reference.

The school uses an Internet Service Provider (ISP) that has filtering software in place to minimise the risk of accessing inappropriate internet material or receiving inappropriate e-mail. Should any children access material they have concerns about, they should notify a member of staff, who will then inform the E-Safeguarding Leader. The Leader will then ask the ICT Technician to inform the ISP of the address of the offending web site. Where possible, appropriate action will then be taken to block further access. On occasions where a total block is not possible, staff will then use this to remind children of their own responsibilities in becoming safe users, in line with the Computing curriculum. The school will take appropriate action against users that use the school facilities to knowingly access, or attempt to access inappropriate materials. Therefore, the school reserves the right to access the work area of any user to view files held in that area.

All children across the school have access to the internet and are able to use the technology available. It is anticipated that access for younger children will be more directed, with autonomous use being available to older children. Where children are given freedom to search the internet for information, they should be given clear learning objectives by their teacher. In the event of inappropriate use or the accessing of inappropriate materials, action will be taken by the teacher, E-Safeguarding Leader or the Headteacher. Any incidents will be reported and logged by the E-Safeguarding Leader.

Children will be taught to use e-mail, the internet and mobile technology responsibly to reduce the risk to themselves and others. After being agreed by staff and children at the beginning of each year, rules for internet access and the use of all technologies within school will be posted in each classroom and around the school. E-Safety will form an integral part of computing lessons but will also be covered in regular assemblies and as part of our PSHE programme of study.

The school believes that access to the internet and mobile devices will enable children to explore resources available from libraries, other schools, LAs and commercial content providers in a way that will enhance the learning process in ways impossible by other means. E-mail will allow communication to be made with other individuals and organisations, regardless of time and distance.

The school believes that access to this technology brings benefits to the learning processes that outweigh the possible risks that might be encountered.

Older children will be encouraged to accept some responsibility for their use of the internet and will be asked to sign a pupil e-safety declaration.

The final responsibility for use of the internet and E-Safety lies with the parents and guardians of our children. Therefore, the school asks parents to sign our Acceptable use Policy and regular e-safety updates. In doing so, parents are giving their permission for their children to be educated in accordance with school policies. Parents will also be provided with support and guidance in maintaining their children's safety away from school, through regular events in school and through documentation provided on our website. Such information will also be available in hard copies from the school, should this be required.

Monitoring and Review

This policy is monitored by the Headteacher, who reports to governors about the effectiveness of the policy on request. It will be reviewed appropriate to new legislation or to the needs of the school.

This policy will be reviewed in April 2020

Signed ____________________________Headteacher Date _________________

Signed ____________________________Chair of Governors Date _________________

Letter to Parents

Dear Parent/Guardian,

Responsible Use of the Internet.

I ask that you read this letter and the attached policy and then sign and return the slip to school.

Millions of people today use the internet and e-mail as part of their daily lives. At Hoylandswaine, we recognise this, and believe our children should have the opportunity to learn about and use these emerging and changing technologies. This will not only help to support their learning across the curriculum but also equip the children with the skills they will require for life-long learning.

In order to develop their learning, our children have regular access to computers, laptops, mobile devices and to the internet throughout the school. We are fully aware of the concerns and issues surrounding safe internet use and have a clear policy in place for dealing with this, a copy of which is attached and would require both your own and your child's signature. Our internet provider is filtered and any computer use is monitored by staff. E-safety rules are agreed by staff and children at the start of each year. These are displayed throughout the school and are available to view on our website.

Should you have any further concerns or wish to discuss any aspect of Internet use, please do not hesitate to contact me at the school.

Yours sincerely,

Mr D Bond
Computing / E-Safeguarding Leader

HOYLANDSWAINE SCHOOL

Acceptable Use Agreement for Pupils using Computers – Key Stage 1

Please could you read through this user agreement with your child.

Once you and your child have signed it, please could you give the agreement back to your child's class teacher.

Failure to send this form back may mean that your child cannot access the Internet or computers in school.

Child's Name: ____________________________

Class Teacher: ___________________________

Rules I must follow to safely use the computers at school

- I will only use the internet when my teacher says I can
- I will listen carefully to all the teachers and follow their instructions
- I will only use the school's computers for my school work
- I will only log on as myself
- I will not have my own e-mail address
- I will turn off the monitor or if I see something that I feel uncomfortable with or upsets me, then I will tell my teacher straight away.
- I will not use unkind words or say things that may hurt other people's feelings when I am at school especially when I am using the computers.

Signature - Pupil: __________________________ Date: __________________

Signature - Parent: _________________________ Date: __________________

HOYLANDSWAINE SCHOOL

Acceptable Use Agreement for Pupils using Computers – Key Stage 2

Please could you read through this user agreement with your child.

Once you and your child have signed it, please could you give the agreement back to your child's class teacher.

Failure to send this form back may mean that your child cannot access the Internet or computers in school.

Child's Name: ____________________________

Class Teacher: ___________________________

Rules I must follow to safely use the computers at school

- I will only use ICT in school for school purposes.
- I will only use the internet when my teacher says I can
- I will listen carefully to all the teachers and follow their instructions
- I will only use the school's computers for my school work
- I will only log on as myself
- I will only open/delete my own files.
- I will not tell other people my ICT passwords.
- I will only open message attachments from people I know, or who my teacher has approved.
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this, I will tell my teacher or an adult in school immediately.

- I will not give out my own details such as my name, phone number or home address. I will not arrange to meet someone.

- I will turn off the monitor or if I see something that I feel uncomfortable with or upsets me, then I will tell my teacher straight away.

- I will not use unkind words or say things that may hurt other people's feelings when I am at school especially when I am using the computers.

- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.

- I know that my use of ICT can be checked and that my parent/carer contacted if a member of school staff is concerned about my e-Safety.

Signature - Pupil: ___________________________ Date: ___________________

Signature - Parent: __________________________ Date: ___________________

Hoylandswaine Primary School

STAFF, GOVERNOR AND VISITOR ACCEPTABLE USE AGREEMENT

ICT and the related technologies such as e-mail, the Internet and mobile devices are an expected part of our daily working life in school. This policy is to help ensure that all staff are aware of their professional responsibilities when using any form of ICT and to help keep staff, governors and visitors safe. All staff are expected to sign this policy confirming their undertaking to adhere to its contents at all times. Any concerns or clarification should be discussed with the Designated Persons for E-Safety (Mr Damien Bond) and the Headteacher (Mrs Laura Cole).

- The laptops and software are school property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.
- I will look after equipment loaned to me and for insurance purposes I will not leave it unattended in a car.
- I will only use the school's e-mail/Internet/Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Headteacher or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role and through official school systems.
- I will only use the approved e-mail system for any communications with pupils, parents and other school related activities.
- I will ensure that data of a personal or sensitive nature such as that stored within the school administration system is kept secure and accessed appropriately. Personal or sensitive data can only be taken off school premises or accessed remotely if protected by appropriate technical controls agreed by the Headteacher and the Governing Body.
- I will not give out my own personal details, such as mobile phone number or personal e-mail address, to pupils.
- I will not install any hardware or software on school equipment without the permission of the Headteacher.
- I will report **any** incident relating to the use of technology or otherwise to the appropriate delegated person within school immediately.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/or staff will only be taken, stored and used for professional purposes in line with data protection policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/carer, member of staff or Headteacher in line with GDPR.
- I understand that the Headteacher may authorise my use of the Internet and other related technologies.
- I will respect copyright and intellectual property rights.
- **I will ensure that my online activity, both in school and outside school, will not bring my professional role into dispute. This includes ignoring invitations from pupils and parents to be part of their social networking sites. My private social networking will not be linked to or with my professional role.**
- I will report any incidents of concern regarding pupils' safety to the Headteacher immediately.
- I will support and promote the school's e-safeguarding policy and help pupils to be safe and responsible in their use of ICT and related technologies. I am aware that e-safety logs are in the staffroom and in the first instance these should be completed and given to the designated person for e-safeguarding.

The school will exercise its right to monitor the use of the school's information systems including internet access, interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the system may be taking place or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound. The misuse of ICT or failing to comply with the Acceptable Use Agreement may lead to disciplinary action which in turn may lead to dismissal.

User Signature I agree to follow this Acceptable Use Agreement and to support the safe use of ICT in the school.

Name ________________________________ Signature ________________ Date ____________

(Reviewed September 2018)