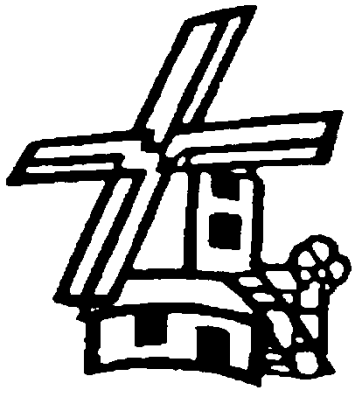
Millfields Primary School

# E-Safety and Acceptable ICT Use Policy

**Signed: Chair of Governors ……David Roscoe**

**Date ……23/11/2017**

**Review date ……November 2020**



# Safeguarding and PREVENT Statement

At Millfields Primary 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 Millfields Primary 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.

As of July 2015, the Counter-Terrorism and Security Act (HMG, 2015) placed a new duty on schools and other education providers. Under section 26 of the Act, schools are required, in the exercise of their functions, to have "due regard to the need to prevent people from being drawn into terrorism". This duty is known as the Prevent duty.

It requires schools to:

- teach a broad and balanced curriculum which promotes spiritual, moral, cultural, mental and physical development of pupils and prepares them for the opportunities, responsibilities and experiences of life and must promote community cohesion
- be safe spaces in which children / young people can understand and discuss sensitive topics, including terrorism and the extremist ideas that are part of terrorist ideology, and learn how to challenge these ideas
- be mindful of their existing duties to forbid political indoctrination and secure a balanced presentation of political issues

Millfields Primary School works in accordance with the PREVENT Duty and treats this issue as seriously as any other child protection matter.

## Scope of the Policy

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

The school will deal with cyber-bullying and other e-safety 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 both in and out of school.

## Roles and Responsibilities

The following section outlines the e-safety roles and responsibilities of individuals and groups within Millfields Primary School:

Governors:
Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy.

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 head should be 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).
• The Headteacher is 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.

E-Safety Coordinator / Officer:
• 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
• liaises with the Local Authority / relevant body
• liaises with school technical staff
• receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments.

Network Manager
• the school's technical infrastructure is secure and is not open to misuse or malicious attack
• the school meets required e-safety technical requirements and that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
• the broadband filter from Essex Broadband Services is applied at the appropriate level for the user and that this is updated/checked regularly.

Teaching and Support Staff:
• they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
• they report any suspected misuse or problem to the Headteacher/E-Safety Coordinator
• all digital communications with parents /carers should be on a professional level and only carried out using official school systems, with the exception of the use of mobile phones for contact during school trips
• e-safety issues are embedded in all aspects of the curriculum and other activities
• pupils understand and follow the e-safety and acceptable use policies
• they monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other 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 / Safeguarding 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:
• are responsible for using the school digital technology systems respectfully and safely
• need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
• will be expected to know and understand safe use of mobile devices and digital cameras; they should also know and understand about use of images and cyber-bullying.
• 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. Millfields will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website / Millfields (Official) Facebook page and information about e-safety campaigns. Parents and carers will be encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of:
• digital and video images taken at school events
• access to parents' sections of the website

## Policy Statements

Education – students / 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 therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.
E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum. The e-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities. It will be provided in the following ways:
• A planned e-safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited
• Pupils should be taught to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
• Staff should act as good role models in their use of digital technologies, the internet and mobile devices
• In lessons where internet use is pre-planned, it is best practice that 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.
• Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
• It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Education – parents / carers
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.

Millfields will therefore seek to provide information and awareness to parents and carers through:
• Letters, newsletters, web site
• Parents / Carers sessions
• High profile events / campaigns eg Safer Internet Day
• Reference to the relevant web sites / publications

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 formal e-safety training will be made available to staff. This will be regularly updated and reinforced.
• 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
• The E-Safety Coordinator will provide advice / guidance / training to individuals as required.

Training – Governors
Governors should take part in e-safety training / awareness sessions. This may be offered in a number of ways:
• Attendance at training provided by the Local Authority / National Governors Association / or other relevant organisation
• Participation in school training / information sessions for staff or parents

## Technical – infrastructure / equipment, filtering and monitoring

Millfields has a managed ICT service provided by an outside contractor and it is the responsibility of the school to ensure that the managed service provider carries out all the e-safety measures that would otherwise be the responsibility of the school.
Millfields is responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented.

Millfields' technical systems will be managed in ways that ensure that the school meets recommended technical requirements

• Servers, wireless systems and cabling must be securely located and physical access restricted

• All users will have clearly defined access rights to school technical systems and devices.

• All staff users will be provided with a username and secure password by technician/Computing lead who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password.

• The "administrator" passwords for the school ICT system, used by the Network Manager/Computing lead must also be available to the Headteacher / Principal or other nominated senior leader and kept in a secure place (e.g. school safe)

• Technician/Computing lead are 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 installation

•Internet access is filtered for all users. Illegal content (e.g. child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list.

• The school has provided differentiated user-level filtering

• An appropriate proforma is available for users to report any actual / potential technical incident / security breach to the relevant person.

• 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. The school infrastructure and individual workstations are protected by up to date virus software.

• There is provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school systems.

• Staff are allowed to use cameras and laptops out of school and must sign any other equipment out. Family members and friends must not use this equipment.

• Staff are able to download executable files and install programmes on school devices but will need permission and the password put in for them.

•. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

## Bring Your Own Device (BYOD)

The educational opportunities offered by mobile technologies are being expanded as a wide range of devices, software and online services become available for teaching and learning, within and beyond the classroom. This has led to the exploration by schools of users bringing their own technologies in order to provide a greater freedom of choice and usability. Use of BYOD should not introduce vulnerabilities into existing secure environments. Considerations will need to include; levels of secure access, filtering, data protection, storage and transfer of data, mobile device management systems, training, support, acceptable use, auditing and monitoring.

- The school has a set of clear expectations and responsibilities for all users
- The school adheres to the Data Protection Act principles
- All users are provided with and accept the Acceptable Use Agreement
- All network systems are secure and access for users is differentiated
- Where possible these devices will be covered by the school's normal filtering systems, while being used on the premises
- All users will use their username and password and keep this safe

## 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 cyberbullying 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 accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use. To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites. Parents/carers should only make positive and encouraging comments 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, if including children, should only be taken on school equipment; the personal equipment of staff or volunteers 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, on the school Facebook page, 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 Facebook entry, particularly in association with photographs.
• Written permission from parents or carers will be obtained before photographs of pupils are published on the school website or on the school Facebook page.

## 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.

Millfields 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". (see Privacy Notice section in the appendix)
- It has a Data Protection Policy
- 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

- There are clear policies about the use of cloud storage / cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner's Office.

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, 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 (below) once it has been transferred or its use is complete

## Communication

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

| | Staff and other adults | | | | Pupils | | | |
|---|---|---|---|---|---|---|---|---|
| **Communication and technology** | Allowed | Allowed at certain times | Allowed for selected staff | Not allowed | Allowed | Allowed at certain times | Allowed with staff permission | Not allowed |
| Mobile phones may be brought to school | X | | | | X* | | | |
| Use of mobile phones in lessons | | | | X | | | | X |
| Use of mobile phones in social time | X | | | | | | | X |
| Taking photos of children on mobile phones / cameras from home | | | | X | | | | X |
| Use of other mobile devices eg tablets, gaming devices | | X | | | | X | | |
| Use of personal email addresses in school, or on school network | X | | | | | | | X |
| Use of school email for personal emails | | | | X | | | | X |
| Use of messaging apps | | X | | | | | | X |
| Use of social media | | X | | | | | | X |
| Use of blogs | X | | | | | X | | |

* Needs to be put in the school office for the day

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 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 students / pupils or parents / carers (email, chat, Facebook etc.) must be professional in tone and content.

• Pupils should be taught about e-safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.

• Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

## Social Media - Protecting Professional Identity

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 the school or local authority
- Security settings are on

## Unsuitable / inappropriate 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 school or outside school when using school equipment or systems. The school policy restricts usage as follows:

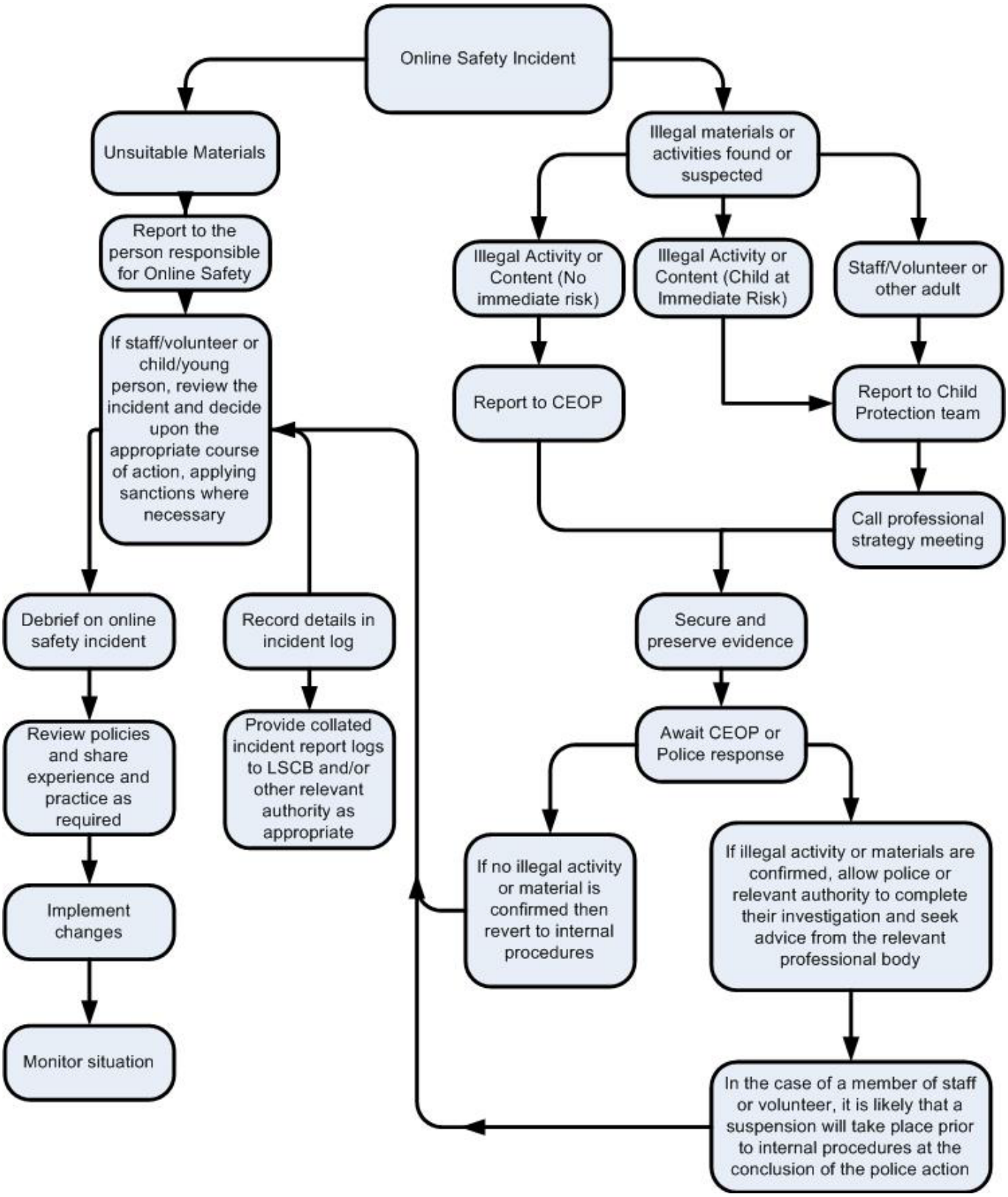
| Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to: | Acceptable | Acceptable at certain times | Acceptable for nominated users | Unacceptable | Unacceptable and illegal |
|---|---|---|---|---|---|
| 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 | |
| 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 | | | | 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 on school equipment | | | | X | |
| On-line gambling on personal equipment in school time | | 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 | X | | | | |

# Responding to incidents of misuse

## 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 (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 the school's 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 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 as follows:

Student:

These will be dealt in the first instance by the class teacher and then if necessary by the headteacher. Incidents of inappropriate misuse that will need to be dealt with include:

- Unauthorised use of non-educational sites during lessons
- Unauthorised downloading or uploading of files
- Attempting to access or accessing the school network, using the account of a member of staff
- Corrupting or destroying the data of other users
- Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature
- Actions which could bring the school into disrepute or breach the integrity of the ethos of the school
- Accidentally accessing offensive or pornographic material and failing to report the incident
- Deliberately accessing or trying to access offensive or pornographic material

Staff

These incidents will be dealt with by the headteacher and then if necessary refered on to either the LA or police. These incidents include:

- Deliberately accessing or trying to access material that could be considered illegal
- Inappropriate personal use of the internet / social media / personal email
- Unauthorised downloading or uploading of files
- 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
- Careless use of personal data eg holding or transferring data in an insecure manner
- Deliberate actions to breach data protection or network security rules
- Corrupting or destroying data of other users or causing deliberate damage to hardware or software
- Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature
- Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils
- Actions which could compromise the staff member's professional standing
- Actions which could bring the school into disrepute or breach the integrity of the ethos of the school
- Using proxy sites or other means to subvert the school's filtering system

- Accidentally accessing offensive or pornographic material and failing to report the incident
- Deliberately accessing or trying to access offensive or pornographic material
- Breaching copyright or licensing regulation

# Appendices

# Parent / Carer Acceptable Use Agreement

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 Millfields Primary School's 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 try to ensure that pupils will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users.

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

# Permission Form

Parent / Carers Name _____

Student / 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 know that my son / daughter and has received, or 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.

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:_____

# Staff (and Volunteer) Acceptable Use Policy Agreement

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

**This Acceptable Use Policy is intended to ensure:**

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

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

# Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that students / pupils receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

**For my professional and personal safety:**

• I understand that the school will monitor my use of the ICT systems, email and other digital communications.
• I understand that the rules set out in this agreement also apply to use of school ICT systems (e.g. laptops, email, VLE etc.) out of school, and to the transfer of personal data (digital or paper based) out of school
• I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
• I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
• I will immediately report any illegal, inappropriate or harmful material or incident I become aware of, to the appropriate person.

**I will be professional in my communications and actions when using school ICT systems:**

• I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
• I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
• I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (eg on the school website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.
• I will only use chat and social networking sites in school in accordance with the school's policies.
• I will only communicate with students / pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner. (schools should amend this section to take account of their policy on communications with students / pupils and parents / carers. Staff should be made aware of the risks attached to using their personal email addresses / mobile phones / social networking sites for such communications)
• I will not engage in any on-line activity that may compromise my professional responsibilities.

**The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the *school / academy*:**

• When I use my mobile devices (PDAs / laptops / mobile phones / USB devices etc.) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.

• I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)

• I will ensure that my data is regularly backed up.

• I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.

• I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.

• I will not disable or cause any damage to school / academy equipment, or the equipment belonging to others.

• I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School / Academy / LA Personal Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.

• I understand that data protection policy requires that any staff or pupil data, to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.

• I will immediately report any damage or faults involving equipment or software, however this may have happened.

**When using the internet in my professional capacity or for school sanctioned personal use:**

• I will ensure that I have permission to use the original work of others in my own work

• Where work is protected by copyright, I will not download or distribute copies (including music and videos).

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

• I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school

• I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action.

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

Staff/Volunteer name:_____

Signed: _____

Date:_____

# Acceptable Use Agreement for Community Users

**This Acceptable Use Agreement is intended to ensure:**

• that community users of school digital technologies will be responsible users and stay safe while using these systems and devices

• that school systems, devices and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

• that users are protected from potential risk in their use of these systems and devices

**Acceptable Use Agreement**

I understand that I must use school systems and devices in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems, devices and other users. This agreement will also apply to any personal devices that I bring into the school

• I understand that my use of school systems and devices and digital communications will be monitored

• I will not use a personal device that I have brought into school for any activity that would be inappropriate in a school setting.

• I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.

• I will immediately report any illegal, inappropriate or harmful material or incident I become aware of, to the appropriate person.

• I will not access, copy, remove or otherwise alter any other user's files, without permission.

• I will ensure that if I take and / or publish images of others I will only do so with their permission. I will not use my personal equipment to record these images, without permission. If images are published it will not be possible to identify by name, or other personal information, those who are featured.

• I will not publish or share any information I have obtained whilst in the school on any personal website, social networking site or through any other means, unless I have permission from the school.

• I will not, without permission, make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.

• I will not install or attempt to install programmes of any type on a school device, nor will I try to alter computer settings, unless I have permission to do so.

• I will not disable or cause any damage to school equipment, or the equipment belonging to others.

• I will immediately report any damage or faults involving equipment or software, however this may have happened.

• I will ensure that I have permission to use the original work of others in my own work

• Where work is protected by copyright, I will not download or distribute copies (including music and videos).

• I understand that if I fail to comply with this Acceptable Use Agreement, the school has the right to remove my access to school systems / devices

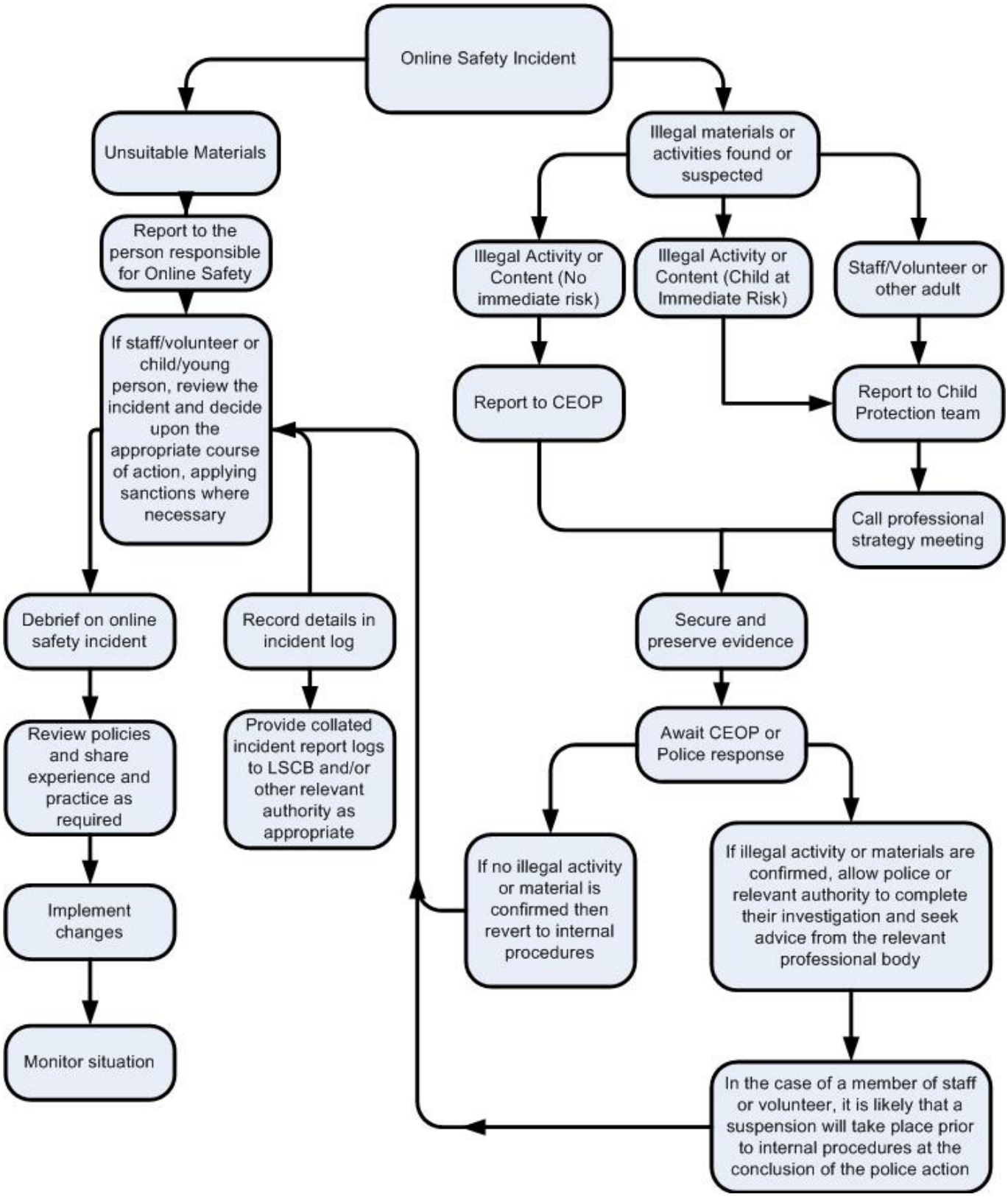
I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Name:_____

Signed: _____

Date:_____

# Responding to incidents of misuse – flow chart



# Reporting E-Safety Concerns Proforma

| | | | |
|---|---|---|---|
| **Person Reporting Concern:** | | **Date:** | |
| **Form Completed by:** | | **Role:** | |
| **Indicate type of incident – please tick below.** | | | |
| **Website** | | **Safeguarding** | |
| Inappropriate website accessed | | Cyber Bullying | |
| Inappropriate behaviour using ICT | | Sexual exploitation using technology | |
| Illegal content accessed | | | |
| Inappropriate use of email or other technologies | | | |
| Deliberate misuse of school network | | | |
| Other | | | |
| **Brief description of concern:** | | | |
| **Action taken:** | | | |
| **Signed:** | | **Date:** | |