Malmesbury Park Primary School
E-Safety Policy
(Adopted: March 2016 – Review March 2017)

Applies to: All Staff	**Pages:** 18	**Ref:**001
Written by: Sue Saxby & Adrian Vivian	**Issue Number:**2	**Date:** March 2016
Approved by: Curriculum and Standards Committee		

School aims and values which guide this policy:

- We work together to make learning purposeful and rewarding
- Learners will develop independence to achieve their full potential
- We are a caring community that promotes respect for self, others and our environment
- We create a supportive learning environment that develops confidence

Terms:
ICT- Information and Communications Technology
PSHE – Personal Social and Health Education
LA – Local Authority
CEOP – Child Exploitation Online Protection
SIRO – Senior Information Risk Officer

Links to other policies:

- Behaviour Management Policy
- Counter-Bullying Policy
- Safeguarding Policy

Introduction:

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment. Malmesbury Park takes the safety of all children and adults very seriously. This policy is written to protect all adults and children.

Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school.

Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Learning Platforms and Virtual Learning Environments
- E-mail and Instant Messaging
- Chat Rooms and Social Networking

- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

This e –safety policy should recognise and seek to develop the skills that children and young people need when communicating and using these technologies properly, while keeping safe and secure, and acting with respect for others.

This policy, supported by the school's acceptable use agreements for staff, governors, visitors and pupils, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: child protection, health and safety, home–school agreements, and behaviour/pupil discipline (including the anti-bullying) policy and PSHE

Roles and Responsibilities

As eSafety is an important aspect of strategic leadership within the school, the Head and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named eSafety co-ordinator in this school is Sue Saxby (Deputy Headteacher) who has been designated this role as a member of the senior leadership team. All members of the school community have been made aware of who holds this post. It is the role of the eSafety co-ordinator to keep abreast of current issues and guidance through organisations such as Bournemouth LA, Becta, CEOP (Child Exploitation and Online Protection) and Childnet.

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

Governors

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of E-Safety within the role of Safeguarding Governor. The role of the E-Safety Governor will include:

- regular meetings with the E-Safety Co-ordinator
- regular monitoring of e-safety incident logs
- regular monitoring of filtering /change controls
- reporting to relevant Governors committee / meeting

Headteacher and Senior Leaders

- The Headteacher has a duty of care for ensuring the safety (including e-safety) of members of the school community

- The Headteacher and (at least) another member of the Senior Leadership Team 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.
- The Headteacher and Senior Leaders are responsible for ensuring that the E-Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The Headteacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

E-Safety Coordinator

- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provides training and advice for staff
- 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,
- meets regularly with E-Safety Governor to discuss current issues, review incident logs
- attends relevant meeting / committee of Governors

Network Manager / Technical staff

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required e-safety technical requirements and any Local Authority / other relevant body e-Safety Policy / Guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- filtering is applied and updated on a daily basis by the internet provider. It's implementation is not the sole responsibility of any single person
- that they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- that the use of the network / internet / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher, E-Safety Coordinator

Teaching and Support Staff

are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem to the Headteacher for investigation / action / sanction
- all digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official school systems
- e-safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the e-safety and acceptable use policies
- pupils have a good understanding of research skills and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) 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

Designated Safeguarding Lead

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 in an acceptable and appropriate manner (following good practice guidelines)
- have a good understanding of research skills and to uphold copyright regulations
- 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 policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety 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. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national / local e-safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good e-safety practice and to follow school e safety guidelines

- Parents/ carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to school
- Parents/ carers are expected to sign a Home School agreement containing the following statement or similar
- Parents/ carers are reminded of the appropriate use of digital and videos taken at school events
-

Parents are regularly reminded of the **school approach to on-line safety and that is to not deliberately upload or add any images, sounds or text that could upset or offend any member of the school community**

E-Safety in the curriculum

ICT and online resources are increasingly used across the curriculum. We believe it is essential for eSafety guidance to be given to the pupils on a regular and meaningful basis. eSafety is embedded within our curriculum and we continually look for new opportunities to promote eSafety. This policy will be successful with effective implementation; ensuring staff remain vigilant in planning and supervising appropriate educational ICT experiences.

- We endeavour to embed eSafety messages across the curriculum whenever the internet and/or related technologies are used
- The eSafety policy will be introduced to the pupils at the start of each school year

- eSafety posters will be prominently displayed around the school and through the school website and internal intranet page
- The school has a framework for teaching internet skills in ICT/ PSHE lessons which can be found within the ICT scheme of work. The scheme of work 'Digital Literacy and Citizenship' from the South West Grid For learning is each half term in every year group at Malmesbury Park.
- Educating pupils on the dangers of technologies that maybe encountered outside school is done informally when opportunities arise and as part of the eSafety curriculum
- Pupils are aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them
- Pupils are taught about copyright and respecting other people's information, images, etc through discussion, modelling and activities
- Pupils are aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Childline or CEOP report abuse button
- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the ICT curriculum.
- Where students / pupils are allowed to freely search the internet, staff will be vigilant in monitoring the content of the websites the young people visit.
- In lessons where internet use is pre-planned, it is best practice that students / 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.
- 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 (or other relevant designated person) 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.

Equal Opportunities

Pupils with additional needs

The school endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the schools' eSafety rules.

However, staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of eSafety issues.

Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of eSafety. Internet activities are planned and well managed for these children and young people.

E-Safety skills development for staff

- Our staff receive regular information and training on eSafety issues in the form of HT bulletins, staff meetings and inset days. Designated staff including the E Safety Champion and ICT coordinator attend specific and regular E safety training.

- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of eSafety and know what to do in the event of misuse of technology by any member of the school community (see enclosed flowchart)

Managing the internet

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. Whenever any inappropriate use is detected it will be followed up.

- The school maintains students who will have supervised access to Internet resources (where reasonable) through the school's fixed and mobile internet technology
- Staff will preview any recommended sites before use
- Raw image searches are discouraged when working with pupils. Google images is the recommended search engine for images in school, providing the highest level of filtering.
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research
- All users must observe copyright of materials from electronic resources
- The school infrastructure and individual workstations are protected by up to date virus software.

In a perfect world, inappropriate material would not be visible to pupils using the Internet, but this is not easy to achieve and cannot be guaranteed. It is a sad fact that pupils may occasionally be confronted with inappropriate material, despite all attempts at filtering. Pupils should be taught what to do if they experience material that they find distasteful, uncomfortable or threatening. For example: to close the page and report the incident immediately to the teacher

Internet Use

- You must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise its intended restricted audience
- Don't reveal names of colleagues, customers or clients or any other confidential information acquired through your job on any social networking site or blog
- On-line gambling or gaming is not allowed

It is at the Headteacher's discretion on what internet activities are permissible for staff and pupils and how this is disseminated.

Managing Social Networking

Social networking sites, if used responsibly both outside and within an educational context can provide easy to use, creative, collaborative and free facilities. However it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our pupils to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

- The school denies access to social networking sites to pupils and staff. The school does not hold any social networking accounts in its name
- All pupils are educated about the potential dangers of information given by others on sites, for example users not being who they say they are.
- Staff are expected to report any notable activity concerning Malmesbury Park to the headteacher or ICT technician
- Staff and children are made aware that they are responsible for the content they publish on social networking sites, forums, blogs, wikis or any other form of user-generated media

- Pupils are taught to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online
- Pupils are always reminded to avoid giving out personal details on such sites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, IM/ email address, specific hobbies/ interests)
- Our staff and pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals
- Staff and pupils are encouraged to report any incidents of bullying to the school

Password security

Password security is essential for staff, particularly as they are able to access and use pupil data. Staff are expected to have secure passwords which are not shared with anyone. The pupils are expected to keep their passwords secure and not to share with others, particularly their friends. Staff and pupils are regularly reminded of the need for password security.

- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's e-safety Policy and Data Security
- Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks, MIS systems, including ensuring that passwords are not shared and are changed every 30 days. Individual staff users must also make sure that workstations are not left unattended and are locked. The automatic lock time for the school computers is 15 minutes.
- Passwords have to meet the requirements enforced by the network. This is currently more than 5 characters long and unique for each new password changed. A designated user name and password is provided for guests or external trainers to the school.
- Do not record passwords or encryption keys on paper or in an unprotected file
- Change passwords whenever there is any indication of possible system or password compromise
- 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.

Data security

The accessing and appropriate use of school data is something that the school takes very seriously.

The school follows:

- Becta guidelines Becta Schools - Leadership and management - Security - Data handling security guidance for schools (published Spring 2009) and the Local Authority guidance documents listed below
- HGfL: School Admin: School Office: Data Protection and Freedom of Information
- Headteacher's Guidance – Data Security in Schools – Dos and Don'ts
- Network Manager/MIS Administrator or Manager Guidance – Data Security in Schools
- Staff Guidance – Data Security in Schools – Dos and Don'ts
- SIRO/IAO Guidance – Data Security in Schools - Dos and Don'ts

Infrastructure – Monitoring and filtering

All internet activity is logged by the school's internet provider (Virgin Media.)

- A further level of monitoring (websites visited; Users logged in and email use) is carried out by our school ICT Technician.

- Any policy breach is grounds for disciplinary action in accordance with the School Disciplinary Procedure.
- Policy breaches may also lead to criminal or civil proceedings.
- Malmesbury Park Primary School is aware of its responsibility when monitoring staff communication under current legislation and takes into account; Data Protection Act 1998, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998
- Pupils and Staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is not the school's responsibility nor the network manager's to install or maintain virus protection on personal systems. If pupils wish to bring in work on removable media it must be given to the teacher for a safety check first
- Pupils and staff are not permitted to download programs or files on school based technologies without seeking prior permission from the Headteacher or ICT Technician.
- If there are any issues related to viruses or anti-virus software, the network manager should be informed
- Hardware may only be disposed of following consultation with the ICT technician and/or head teacher

Protecting Personal, Sensitive, Confidential and Classified Information

- Ensure that any school information accessed from your own PC or removable media equipment is kept secure.
- Ensure the accuracy of any personal, sensitive, confidential and classified information you disclose or share with others
- Ensure that personal, sensitive, confidential or classified information is not disclosed to any unauthorised person
- Only download personal data from systems if expressly authorised to do so by your manager
- You must not post on the internet personal, sensitive, confidential, or classified information, or disseminate such information in any way that may compromise its intended restricted audience
- Ensure hard copies of data are securely stored and disposed of after use in accordance with the document labelling

Senior Information Risk Officer

The SIRO is a senior member of staff who is familiar with information risks and the school's response. Typically, the SIRO should be a member of the senior leadership team and have the following responsibilities:

- they own the information risk policy and risk assessment
- they appoint the Information Asset Owner(s) (IAOs)
- they act as an advocate for information risk management

The SIRO in this school is the Headteacher

Information Asset Owner.

Any information that is sensitive needs to be protected. This will include the personal data of learners and staff; such as assessment records, medical information and special educational needs data. Schools should identify an Information Asset Owner. As a result, the IAO is able to manage and address risks to the information and make sure that information handling complies with legal requirements.

Although these roles have been explicitly identified, the handling of secured data is everyone's responsibility – whether they are an employee, consultant, software provider or managed service provider. Failing to apply appropriate controls to secure data could amount to gross misconduct or even legal action.

Storing/Transferring Personal, Sensitive, Confidential or Classified Information Using Removable Media.

- Ensure removable media is purchased with encryption. Any sensitive or personal information must be held on an encrypted storage device.
- Store all removable media securely
- Securely dispose of removable media that may hold personal data
- Encrypt all files containing personal, sensitive, confidential or classified data
- Non sensitive or personal data does not need to be stored on an encrypted storage device i.e lesson plans.

Remote Access

- You are responsible for all activity via your remote access facility. Maintain access security at all times at the same level as is used in school.

Mobile technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Many existing mobile technologies such as portable media players, gaming devices, mobile and Smart phones are familiar to children outside of school too. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

Personal Mobile devices (including phones)

- The school allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the school allow a member of staff to contact a pupil or parent/ carer using their personal device
- Pupils are allowed to bring personal mobile devices/phones to school but must not use them for personal purposes within lesson time. The device must be left in the school office for the duration of the school day.
- This technology may be used, however for educational purposes, as mutually agreed with the Headteacher. The device user, in this instance, must always ask the prior permission of the bill payer
- The school is not responsible for the loss, damage or theft of any personal mobile device
- The sending of inappropriate text messages between any member of the school community is not allowed
- Permission must be sought before any image or sound recordings are made on these devices of any member of the school community
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device

	Staff & other adults		Students / Pupils	
Communication Technologies	**Not allowed**	**Allowed**	**Not allowed**	**Allowed**
Mobile phones may be brought to school		Phone not to be used in classrooms or on trip. Access only allowed during own time when in school.		Phone must be left in the school office at the start of the day and collected at the end of the day
Use of mobile phones in lessons	✓		✓	
Use of mobile phones in social time		✓	✓	
Taking photos on mobile phones / cameras	Staff are expected to use school devices for taking photos in school an on trips. Personal devices may be used in very exceptional cases where permission has been sought and images are removed once transferred to the school network. This must be completed in the same day.		Special arrangements will be discussed for individual school trips	
Use of other mobile devices in school eg tablets		Allowed during social time	Special arrangements will be discussed for individual school trips/ homework/home learning	
Use of personal email addresses in school, or on school network		During social time only	✓	
Use of school email for personal emails	✓		✓	
Use of messaging apps		During social time only	✓	
Use of social media	✓		✓	

School provided mobile devices

- The sending of inappropriate text messages between any member of the school community is not allowed
- Permission must be sought before any image or sound recordings are made on the devices of any member of the school community
- Where the school provides mobile technologies such as phones, laptops for offsite visits and trips, only these devices should be used
- Where the school provides a laptop for staff, only this device may be used to conduct school business outside of school

Safe use of images

Taking of images and films

Digital images are easy to capture, reproduce and publish and, therefore, misuse. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.

- With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on field trips. However with the express permission of the Headteacher, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the staff device
- Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of the others, this includes when on field trips. However with the express permission of the Headteacher, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the pupil's device

Publishing pupil's images and work

On a child's entry to the school, all parents/carers will be asked to give permission to use their child's work/photos in a variety of ways related to school activities.

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, e.g. divorce of parents, custody issues, etc.

Parents/ carers may withdraw permission, in writing, at any time. Consent has to be given by both parents in order for it to be deemed valid.

Pupils' full names will not be published alongside their image

Only the Web Manager and office staff has authority to upload to the site.

Storage of images

- Images/ films of children are stored on the school's network.
- Pupils and staff are not permitted to use personal portable media for storage of images (e.g., USB sticks) without the express permission of the Headteacher
- Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network
- The Headteacher and The ICT Team has the responsibility of deleting the images when they are no longer required, or the pupil has left the school

E-mail

- The school gives all staff their own e-mail account to use for all school business as a work based tool
- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary e-mail histories can be traced. The school email account should be the account that is used for all school business
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal e-mail addresses
- Staff sending e-mails to external organisations, parents or pupils are advised to cc. the Headteacher, line manager or designated account
- E-mails created or received as part of your School job will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000.

- Pupils must immediately tell a teacher/ trusted adult if they receive an offensive e-mail. Similarly staff must inform the e safety coordinator/headteacher if an offensive email is received.
- Pupils are introduced to e-mail as part of the ICT Scheme of Work
- Use your own school e-mail account so that you are clearly identified as the originator of a message
- School e-mail is not to be used for personal advertising
- Never open attachments from an untrusted source; Consult your network manager first.

Webcams, CCTV and video conferencing

- The school uses CCTV for security and safety. The only people with access to this are the Headteacher, Site Managers and Office staff. Notification of CCTV use is displayed at the front of the school.
- Webcams in school are only ever used for specific learning purposes, e.g. monitoring hens' eggs
- Video conferencing
- Permission is sought from parents and carers if their children are involved in video conferences and children are supervised by a member of staff
- The school keeps a record of video conferences, including date, time and participants.

Misuse and infringements

Complaints

Complaints and/ or issues relating to eSafety should be made to the eSafety co-ordinator or Headteacher.

Inappropriate material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the eSafety co-ordinator
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the eSafety co-ordinator, depending on the seriousness of the offence; investigation by the Headteacher/ LA, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences (see flowchart)
- Users are made aware of sanctions relating to the misuse or misconduct by having access to this policy, the Ht bulletin and an Induction Programme.

Review procedure

There will be an on-going opportunity for staff to discuss with the eSafety coordinator any issue of eSafety that concerns them

There will be an on-going opportunity for staff to discuss with the SIRO/AIO any issue of data security that concerns them

This policy will be reviewed every (12) months and consideration given to the implications for future whole school development planning

The policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way

Acceptable use agreement: Staff, Governors and Visitors

ICT (including data) 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 designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the school eSafety coordinator or Jackie Green Senior Information Risk Owner.

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head 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.
- I will not give out my own personal details, such as mobile phone number and personal e-mail address, to pupils.
- I will only use the approved, secure e-mail system(s) for any school business.
- I will ensure that personal data (such as data held on MIS software) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body. Personal or sensitive data taken off site must be encrypted.
- I will not install any hardware of software without permission of the Headteacher
- 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 inline with school 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.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Headteacher.
- 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 disrepute.
- I will support and promote the school's e-Safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies.
- I understand this forms part of the terms and conditions set out in my contract of employment.

User Signature

I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school

Signature …… Date ……

Full Name ……(printed)

Job title . . . . . .

Acceptable use agreement: Pupil (Primary)

Primary Pupil Acceptable Use
Agreement / eSafety Rules

- I will only use ICT in school for school purposes.
- I will only use my class e-mail address or my own school e-mail address when e-mailing.
- I will only open e-mail attachments from people I know, or who my teacher has approved.
- I will not tell other people my passwords.
- I will only open/delete my own files.
- 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 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 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 eSafety.

Letter to go to all parents on induction to the school
Dear Parent/ Carer

ICT including the internet, e-mail and mobile technologies, etc. has become an important part of learning in our school. We expect all children to be safe and responsible when using any ICT.

Please read and discuss these eSafety rules with your child and return the slip at the bottom of this page. If you have any concerns or would like some explanation please contact the class teacher.

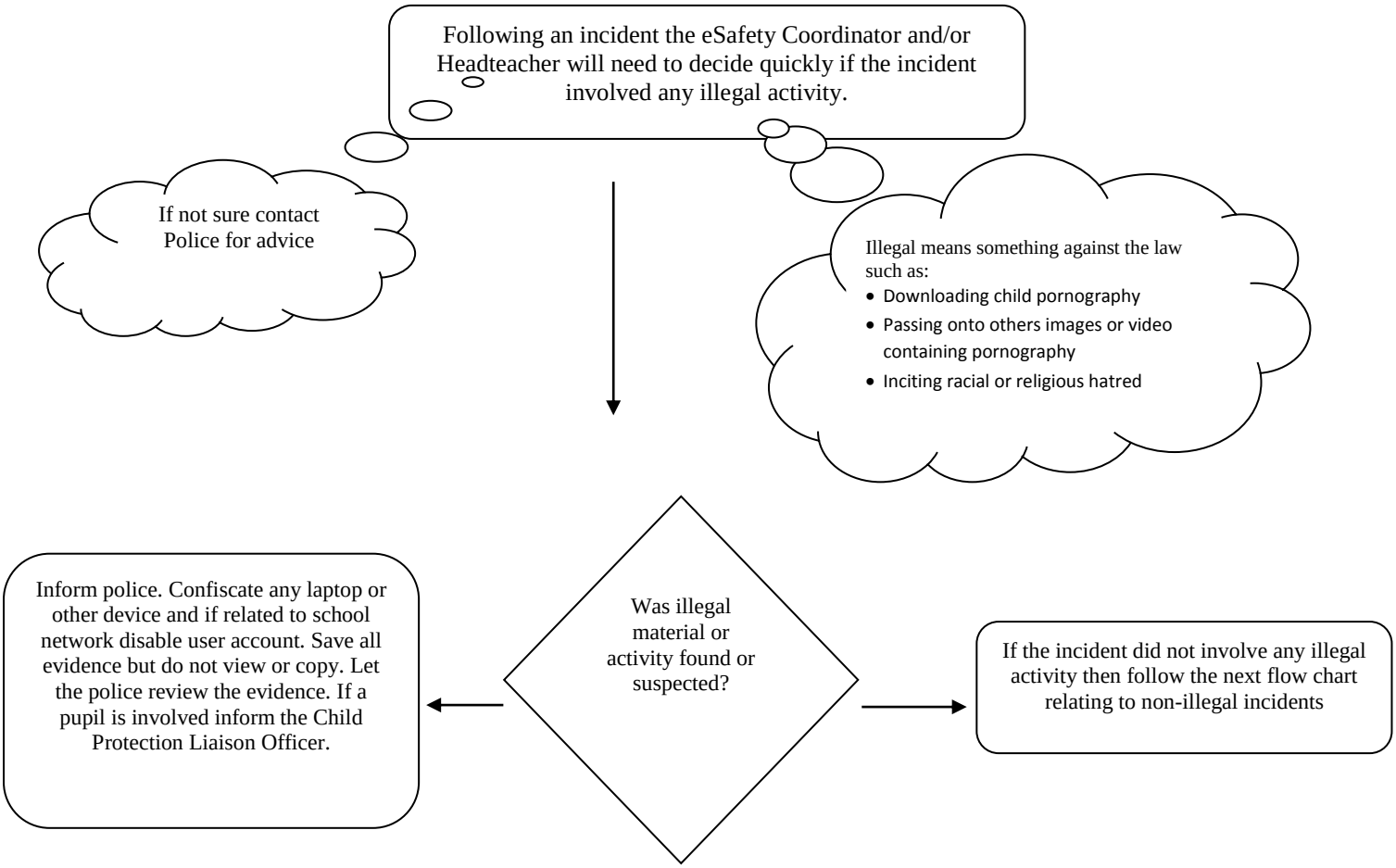
✂----------

Parent/ carer signature
We have discussed this and …….....(child name) agrees to follow the eSafety rules and to support the safe use of ICT at XXX School.

Parent/ Carer Signature …….

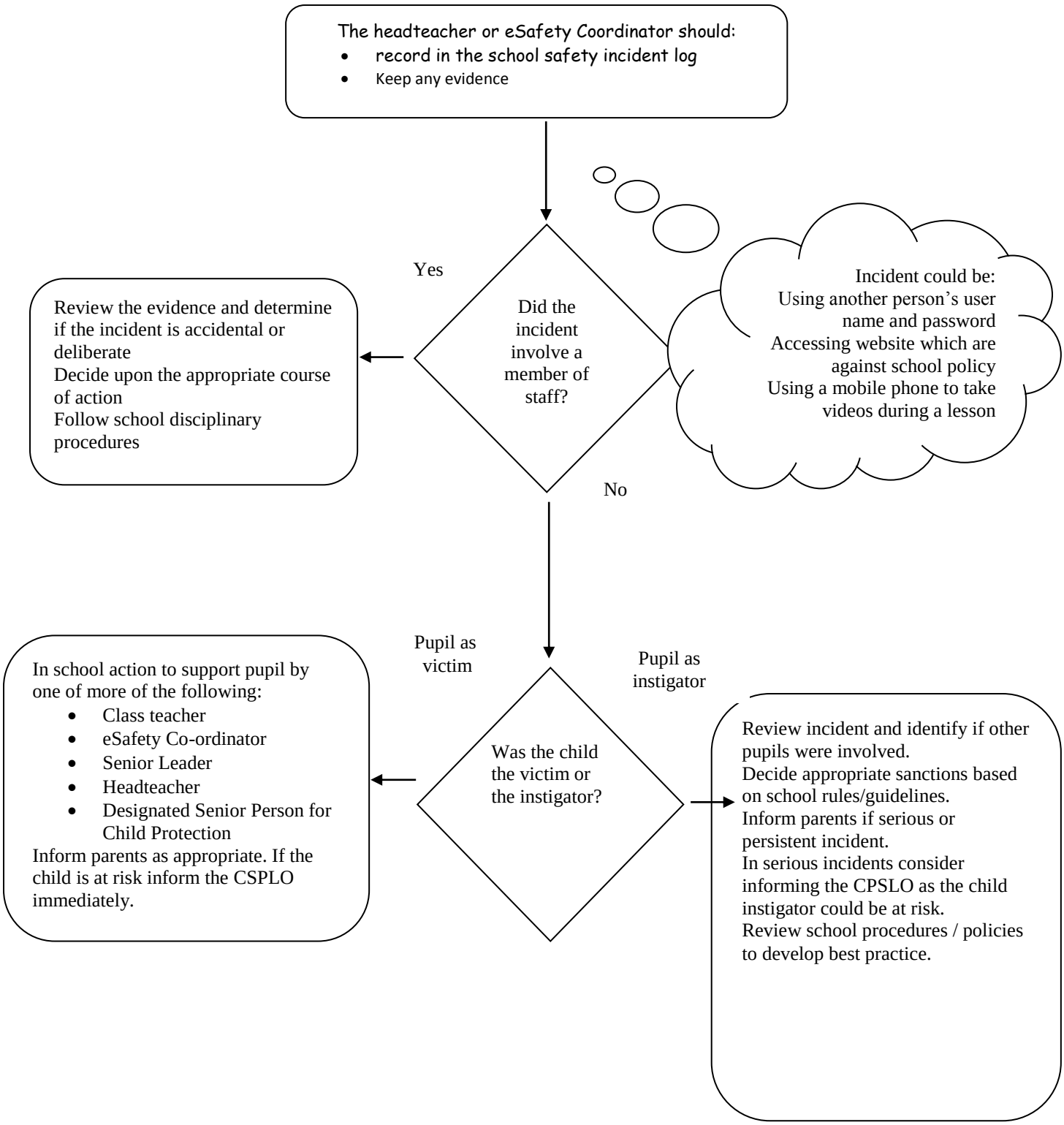
Class ……. Date ……

Flowchart for managing an eSafety incident



Flowchart for managing an eSafety incident

Use this flowchart if the incident did not involve any illegal activity



Incident Log

Incident reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's SIRO or eSafety Co-ordinator. Additionally, all security breaches, lost/stolen equipment or data (including remote access SecureID tokens and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to your Senior Information Risk Owner.

E-Safety Incident Log

Some incidents may need to be recorded in other places, if they relate to a bullying or racist incident.

Malmesbury Park Primary School

E-Safety Incident Log

Details of ALL eSafety incidents to be recorded by the eSafety Coordinator. This incident log will be monitored Termly by the Headteacher, member of SLT or Chair of Governors. Any incidents involving Cyberbullying should be recorded on the school's bullying log.

Date & time	Name of pupil or staff member	Male or female	Room and computer device number	Details of incident (including evidence)	Actions and reasons

Current Legislation

Acts relating to staff emails

Data Protection Act 1998
http://www.hmso.gov.uk/acts/acts1998/19980029.htm

The Telecommunications (Lawful Business Practice)

(Interception of Communications) Regulations 2000
http://www.hmso.gov.uk/si/si2000/20002699.htm

Regulation of Investigatory Powers Act 2000
http://www.hmso.gov.uk/acts/acts2000/20000023.htm

Human Rights Act 1998
http://www.hmso.gov.uk/acts/acts1998/19980042.htm

Other acts relating to eSafety

Racial and Religious Hatred Act 2006

Sexual Offences Act 2003
For more information go to www.education.gov.uk/schools

Communications Act 2003 (section 127)

The Computer Misuse Act 1990 (sections 1 – 3)

Malicious Communications Act 1988 (section 1)

Copyright, Design and Patents Act 1988

Public Order Act 1986 (sections 17 – 29)

Protection of Children Act 1978 (Section 1)

Obscene Publications Act 1959 and 1964

Protection from Harassment Act 1997

Acts relating to the protection of personal data

Data Protection Act 1998
http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1

The Freedom of Information Act 200
http://www.ico.gov.uk/for_organisations/freedom_of_information_guide.aspx