Chilmark and Fonthill Bishop Primary School

Chilmark & Fonthill Bishop Primary School

Online and E-safety Policy

Updated October 2022
Updates/changes
2019 explicit links added to computing curriculum
2020 Links to this policy added to PSHE, RSE curriculum

Background and Rationale

The potential that technology has to impact on the lives of all citizens increases year on year. This is probably even truer for children, who are generally much more open to developing technologies than many adults. In many areas technology is transforming the way that schools teach and that children learn. At home, technology is changing the way children live and the activities in which they choose to partake; these trends are set to continue.

While developing technology brings many opportunities, it also brings risks and potential dangers of which these are just a few;

- access to illegal, harmful or inappropriate images or other content
- unauthorised access to/loss of/sharing of personal information
- the risk of being subject to grooming by those with whom they make contact on the internet
- the sharing/distribution of personal images without an individual's consent or knowledge
- inappropriate communication/contact with others, including strangers
- cyber-bullying and/or peer to peer bullying (see Anti-bullying Policy)
- extremism and radicalisation (see Tackling Extremism and Radicalisation Policy)
- access to unsuitable video / internet games
- an inability to evaluate the quality, accuracy and relevance of information on the internet
- plagiarism and copyright infringement
- illegal downloading of music or video files
- the potential for excessive use which may impact on social and emotional development and learning
- illegal downloading of music or video files
- the potential for excessive use which may impact on social and emotional development and learning.
- online reputations of pupils and peer pressure.

This policy sets out how we strive to keep children safe with technology while they are in school. We recognise that children are often more at risk when using technology at home (where we have no control over the technical structures we put in place to keep them safe) and so this policy also sets out how we educate children of the potential risks. We also explain how we attempt to inform those people who work with our children beyond the school environment (parents/carers and the wider community) to be aware and to assist in this process.

Policy and leadership

This section begins with an outline of the key people responsible for developing our E-safety Policy and keeping everyone safe with computing. It also outlines the core responsibilities of all users of computing in our school.

It goes on to explain how we maintain our policy and then to outline how we try to remain safe while using different aspects of computing.

E-safety is led by the Computing Leader, the Strategic Leadership team and Network Manager who meet regularly to:

- review and monitor any issues relating to school filtering.
- discuss any e-safety issues that have arisen and how they should be dealt with.

Issues that arise are referred to other school bodies as appropriate and when necessary to bodies outside the school such as; Children's Services, Wiltshire Police, the Child Exploitation and Online Protection Centre (CEOP) and the South West Grid for Learning.

Responsibilities in School

Our Computing subject leader is responsible to the Head Teacher and governors for day to day issues relating to e-safety. They will;

• receive notifications from the South West Grid for Learning and take day-to-day responsibility for e-safety issues.
• report regularly to the Head Teacher.
• review the school e-safety policies/documents in line with new guidance and technology.
• ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident.
• provide training and advice for staff and induct new staff on the acceptable use of computing.
• liaise with the Local Authority and other agencies as necessary.
• liaise with school Network Manager.
• attend relevant meetings and committees of the Governing Body and report incident logs and action taken.
• receive appropriate training and support to fulfil their role effectively.
• have responsibility for directing the Network Manager to blocking/unblocking internet sites or users with the school's filtering system.
• maintain detailed logs of any occasions where the school has used its powers of search and deletion of electronic devices.

Responsibilities of Governors

Our governors are responsible for the approval of this policy and for reviewing its effectiveness. This will be carried out by the governors receiving regular information about e-safety incidents and monitoring reports. Governors will;

• request regular feedback from the SLT on the effectiveness of the E-safety policy.
• monitoring e-safety incident logs and challenge leaders as to the effectiveness of action taken.
• monitoring of filtering and hold SLT to account for their actions.
• monitoring logs of any occasions where the school has used its powers of search and deletion of electronic devices.
• ensure that the school involves the appropriate agencies if criminal material is discovered.

Responsibilities of the Head Teacher

The Head Teacher is responsible for ensuring the safety (including e-safety) of members of the school community, though the day-to-day responsibility for e-safety is delegated to the SLT. The Head Teacher will;

• ensure procedures to be followed in the event of a serious e-safety allegation being made against a member of staff (see flow chart on dealing with e-safety incidents).
• ensure relevant disciplinary procedures are followed in the event of serious incidents occurring.
• ensure that the relevant outside agencies are contacted in relation to the nature of the material discovered or the event which has occurred.

Responsibilities of all staff

Teaching and support staff are responsible for ensuring that;

- they have an up to date awareness of e-safety and matters of the current school e-safety policy and practices
- they have read, understood and accepted the school's Responsible Use Policy
- they report and suspected misuse or problem to the SLT.
- e-safety issues are embedded in the Computing and PSHE curriculum and other school activities, such as assemblies.

Responsibilities of the Network Manager and COMPUTING technician(s)

The Network Manager and Computing Technician(s) are responsible for ensuring that;

- the school's computing infrastructure is secure and is not open to misuse or malicious attack.
- users may only access the school's networks through properly enforced password protection.
- shortcomings in the infrastructure are reported to the SLT or Head Teacher so that

appropriate action may be taken.

Schedule for development/monitoring/review of this policy

The implementation of this e-safety policy will be monitored by the SLT under the direction of the Head Teacher. Monitoring will take place at regular intervals by the Governing Body who will receive a report on the implementation of the e-safety policy will include anonymous details of e-safety incidents.
The e-safety policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place.

Responsible Use Policy

All members of the school community are responsible for using the school COMPUTING systems in accordance with the Responsible Use Policy which they will be expected to sign before being given access to school systems.
Responsible use policies are revisited and resigned annually at the start of each school year and amended accordingly in the light of new developments and discussions with the children which take place at the time.
Parents sign once when their child enters the school for permission for use of their child's image (still or moving) by the school, permission for their child to use the schools COMPUTING resources (including the internet) and permission to publish their work.
Staff and pupils also accept the policy every time they log on to computer equipment at school.
Induction policies for all members of the school include this guidance.

Illegal or Inappropriate content/activities and related sanctions

The school believes that the activities listed below are inappropriate in a school context (those in bold are illegal) and that users should not engage in these activities when using school equipment or systems (in or out of school).
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 (**illegal** - The Protection of Children Act 1978)	• Police • School disciplinary procedures (if staff) • Children's Services
Grooming, incitement, 'sexting', arrangement or facilitation of sexual acts against children	• Police • School disciplinary procedures (if staff)

(**illegal** – Sexual Offences Act 2003)	• Children's Services
Possession of extreme pornographic images (**illegal** – Criminal Justice and Immigration Act 2008)	• Police • School disciplinary procedures (if staff)
Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) (**illegal** – Public Order Act 1986)	• Police • School disciplinary procedures (if staff) • Prevent • Counter Terrorism Unit
Pornography – any form of nudity or sexually suggestive materials	• Behaviour policy • School disciplinary procedures (if staff)
Promotion of any kind of discrimination (possibly a breach of The Equality Act 2010)	• Behaviour policy • Consult Equality Policy and guidance • School disciplinary procedures (if staff)
Promotion of racial or religious hatred, radicalisation and/or extremism (**illegal** - Racial and Religious Hatred Act 2006)	• Behaviour policy • Police • Prevent • Counter Terrorism Unit School disciplinary procedures (if staff)
Threatening behaviour, including promotion of physical violence or mental harm (**potentially illegal**)	• Behaviour policy • Police advice should be sought • School disciplinary procedures (if staff)
Any other information which may be offensive to children/colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute	• Behaviour policy • School disciplinary procedures (if staff)

Reporting of e-safety breaches

It is hoped that all members of the school community will be responsible users of COMPUTING, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. This flow chart shows the process that should be followed;

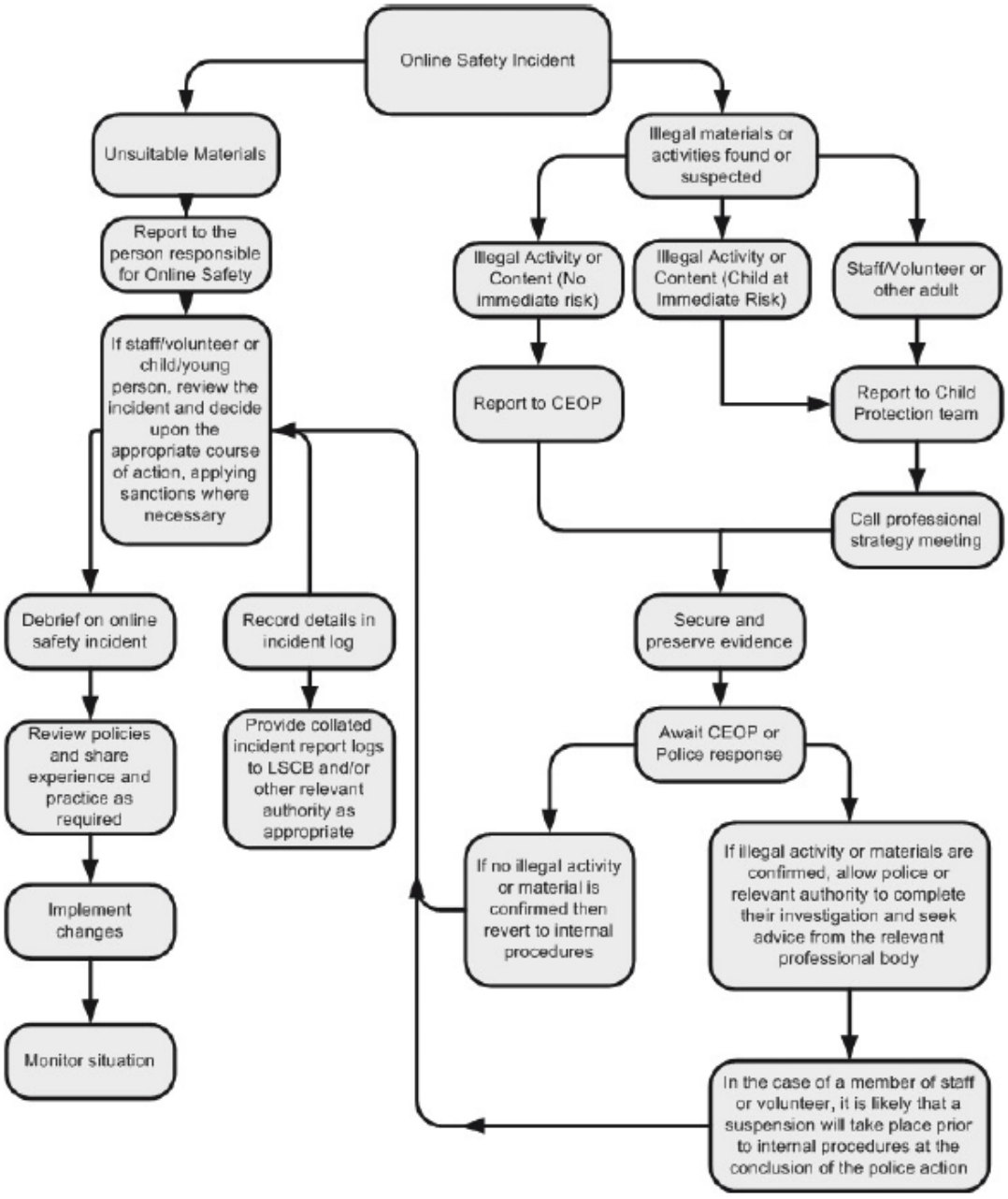
Audit/Monitoring/Reporting/Review

Mobile phones are not allowed in school. The SLT will ensure that full records are kept of incidents involving mobile phones and electronic devices and the deletion of data/files. These records will be reviewed by the Head Teacher / and Governors on a termly basis.

Use of hand held technology by staff (personal phones and hand held devices)
We recognise that the area of mobile technology is rapidly advancing and it is our school's policy to review its stance on such technology on a regular basis. Currently our policy is as follows;

• members of staff are permitted to bring their personal mobile devices into school. Devices must have a locked screen and a password. Members of staff can only use their mobile device in school places where pupils are **not permitted** (i.e. staff room, teachers cupboard).
• pupils are not currently permitted to bring their personal hand held devices into school.

•
a



number of such devices are available in school (e.g. iPads) and are used by children as considered appropriate by members of staff.

Email

Access to email is provided for all users in school via the intranet page accessible via RM Easymail Plus. This is accessible via the web browser (internet Explorer) from their desktop and each teacher has their own private login and password.

These official school email services may be regarded as safe, secure and encrypted and are monitored by RM Easymail Plus.

Staff and pupils should use only the school email services to communicate with others when in school, or on school systems (eg by remote access).

- Staff **MUST NOT** communicate with pupils by email unless specifically authorised to do so by the Head Teacher.
- Staff should inform the SLT if any pupil attempts to make contact with them via email.
- Pupils are informed that they must not attempt to communicate with staff by email unless specifically authorised to do so by the Head Teacher.
- If staff use personal email accounts they must not access them during teaching time and in the presence of pupils. They should be mindful of what they are receiving and sending.
- Users need to be aware that email communications may be monitored.
- Pupils have access to an email account for communication within school.
- A structured education programme is delivered to pupils which helps them to be aware of the dangers of and good practices associated with the use of email.
- Users must immediately report, to their class teacher / SLT – in accordance with the school policy the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.

Use of digital and video images

When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

Members of staff are allowed to take digital still and video images to support educational aims, but must;

• ensure the child(ren) being photographed have parental consent for images to be taken
• follow school policies concerning the sharing, distribution and publication of those images
• only capture images using school equipment; the personal equipment of staff should not be used for such purposes
• take care 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
• not take, use, share, publish or distribute images of others without permission from the Head Teacher
• see also the following section for guidance on publication of photographs.

Use of web-based publication tools

Our school uses the public facing website, for sharing information with the community beyond our school. This includes, from time-to-time celebrating work and achievements of children. All teachers and teaching assistants have an individual username and password so they can publish information on the website. All users are required to consider good practice when publishing content.

• Personal information should not be posted on the school website including official email addresses of staff and pupils
• Only pupil's first names are used on the website, and only then when necessary
• Only calendars of school events relevant to parents/carers are published on the school website
• Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with the following good practice guidance on the use of such images;

Pupils' full names will not be used anywhere on a website or blog, and never in association with photographs.

Filtering- An Introduction

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so. It is therefore important that the school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.

As a school buying internet access, email and technical support services from
The South West Grid for Learning, we automatically receive the benefits of a managed filtering service, tailored specifically for schools.

Responsibilities

The day to day responsibility for the management of the school's filtering is held by the Computing Leader and the SLT (with ultimate responsibility resting with the Head Teacher and Governors). They manage the school filtering, in line with the processes outlined below and keep logs of changes to and breaches of the filtering system.

To ensure that there is a system of checks and balances and to protect those responsible, changes to the standard South West Grid for Learning filtering service must;

• be authorised by more than one responsible person in case there is a breach by one of the responsible persons
• be kept up-to-date with filtering issues that arise
• be monitored and set to send out alerts to the SLT.

Education/training/awareness
Pupils are made aware of the importance of filtering systems through the school's e-safety education programme.

Staff users will be made aware of the filtering systems through:

• signing the RUP (a part of their induction process).
• briefing in staff meetings, training days etc. (from time to time and on-going).

Parents will be informed of the school's filtering policy through the Responsible Use agreement and through safety awareness information in the newsletter etc.

Monitoring
No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network and on school equipment.
Any breaches which are not 'false positive' alerts will be recorded by the Computing leader, along with the action which was taken in response to the breach. This folder is available to be scrutinised by Governors and other agencies as appropriate.

E-safety education
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 safety provision. Children and young people need the help and support of the school to recognise and avoid safety risks and build their resilience. This is particularly important for helping children to stay safe out of school where technical support and filtering may not be available to them.

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

• an e-safety programme should be provided as part of COMPUTING, PHSE and other lessons and should be regularly revisited – this will cover both the use of COMPUTING and new technologies in school and outside school.
• pupils are **NEVER** allowed to use COMPUTING equipment unsupervised.
• we use the resources on CEOP's Think U Know site as a basis for our e-safety education http://www.thinkuknow.co.uk/teachers/resources/ (Hector's World at KS1 and Cyber Cafe at KS2)
• key e-safety messages should be reinforced through further input via assemblies and pastoral activities as well as informal conversations when the opportunity arises.
• pupils take part in Safer Internet Day each year.
• where pupils are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.

Information literacy
Pupils should be taught in all lessons to be critically aware of the content they access online and be guided to validate the accuracy of information by employing techniques such as:

- checking the likely validity of the URL (web address).
- cross checking references (can they find the same information on other sites).
- pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- pupils are taught how to make best use of internet search engines to arrive at the information they require.

We use the resources on CEOP's Think U Know site as a basis for our e-safety education.

Guidance for Reviewing Internet Sites

This guidance is intended for use when the school needs 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 typically include cyber-bullying, harassment, anti-social behaviour and deception. These may appear in emails, texts, social networking sites, messaging sites, gaming sites or blogs etc.

Do not follow this procedure if you suspect that the web site(s) concerned may contain child abuse images. If this is the case please refer to the Flowchart for responding to online safety incidents and report immediately to the police. Please follow all steps in this procedure:

- 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 disciplinary 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.
- Isolate the computer in question as best you can. Any change to its state may affect a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the group, 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.

Documents and relevant legislation

Education Act 1996
Education and Inspections Act 2006
Education Act 2011 Part 2 (Discipline)
The School Behaviour (Determination and Publicising of Measures in Academies) Regulations 2012
Health and Safety at Work etc. Act 1974
Obscene Publications Act 1959
Children Act 1989
Human Rights Act 1998
Computer Misuse Act 1990
This is not a full list of Acts involved in the formation of this advice.