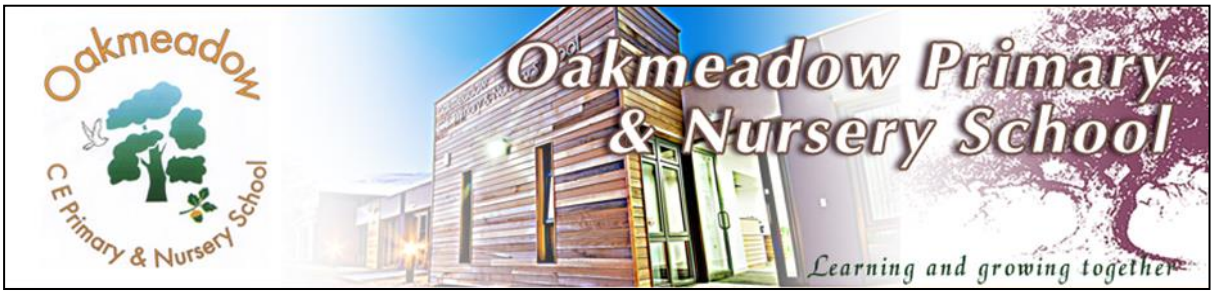
Oakmeadow C.E. Primary & Nursery School

This is a brain stretching, laughter sharing, independence building and mistake making sort of place. Where we have faith and everyone matters!



E-Safety Policy

Reviewed, amended and ratified–Autumn 2017

E-Safety Policy

E-Safety encompasses Internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences.

The school's e-safety policy will operate in conjunction with other policies including those for Pupil Behaviour, Bullying, Curriculum, Data Protection and Security.

Good Habits

E-Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and pupils; encouraged by education and made explicit through published policies.
- Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband from Shropshire LA, through SITTs, for Learning including the effective management of content filtering.
- Secure video and internet links provided through subscription to espresso (espresso providing a dedicated server of secure material updated weekly)
- National Education Network standards and specifications. (The NEN is the UK collaborative network for education, providing schools with a safe, secure and reliable learning environment and direct access to a growing range of online services and content.)

School e-Safety Policy

Oakmeadow's Designated Child Protection Officer will also act as the E-Safety Coordinator as the roles overlap.

Our e-Safety Policy has been written by the school, building on the Shropshire Children and Young Peoples' Directorate and Government guidance. It has been agreed by the senior management team and approved by governors and regularly reviewed.

Designated Safeguarding Lead (DSL): The DSL is trained in E-Safety issues and is aware of the potential for serious child protection issues which can arise from the use of the internet and ICT.

They will act in accordance with the procedures described in the Child Protection Policy should any issue arise, particularly in relation to:

- **Sharing of personal data.**
- **Access to illegal / inappropriate materials.**
- **Inappropriate on-line contact with adults / strangers.**
- **Potential or actual incidents of grooming.**
- **Cyber-bullying.**
- **Sexting.**
- **The Prevent Duty.**

Why is Internet Use important?

The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and administration systems.

Internet use is part of the statutory curriculum and a necessary tool for learning. It is an essential element in 21st century life for education, business and social interaction. Access to the Internet is therefore an entitlement for pupils who show a responsible and mature approach to its use. Our school has a duty to provide pupils with quality Internet access

Pupils will use the Internet outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

How does Internet use benefit education?

Benefits of using the Internet in education include:

- access to world-wide educational resources including museums and art galleries;
- inclusion in the National Education Network which connects all UK schools (The NEN is the UK collaborative network for education, providing schools with a safe, secure and reliable learning environment and direct access to a growing range of online services and content);
- educational and cultural exchanges between pupils world-wide;
- access to experts in many fields for pupils and staff;
- professional development for staff through access to national developments, educational materials and effective curriculum practice;
- collaboration across support services and professional associations;
- improved access to technical support including remote management of
- networks and automatic system updates;
- exchange of curriculum and administration data with the Local Authority and DCSF; access to learning wherever and whenever convenient.

How can Internet Use Enhance Learning?

- The school Internet access will be designed expressly for pupil use and includes filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Internet access will be planned to enrich and extend learning activities.

- Staff should guide pupils in on-line activities that will support learning outcomes planned for the pupils' age and maturity.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Authorised Internet Access

- All staff must read and sign the '**Acceptable ICT Use Agreement'** before using any school ICT resource.

World Wide Web

- If staff or pupils discover unsuitable sites, the URL (address), time, content must be reported to the T&W helpdesk via the e-safety coordinator or other senior member of staff. ***The school has a security system which tracks appropriate use and misuse will result in conduct review with the head teacher.***
- Pupils should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.

Curriculum:
 Where pupils are allowed to search the Internet, eg using search engines, staff are vigilant in monitoring the content of the websites the young people visit and encourage pupils to use specific appropriate search terms to reduce the likelihood of coning across unsuitable material.
 Pupils are taught to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
 Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the Internet

Email

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Access in school to external personal e-mail accounts may be blocked.
- E-mail sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.

Social Networking (reference the social media policy alongside this)

- The School will block/filter access to social networking sites and newsgroups unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location
- Pupils should be advised not to place personal photos on any social network space.
- Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Pupils should be encouraged to invite known friends only and deny access to others.

Use of Digital and Video Images - Photographic, Video

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 and pupils / pupils need to be aware of the risks associated with sharing images and with posting digital images on the Internet.

Those images may remain available on the Internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out Internet searches for information about potential and existing employees. The school informs and educates users about these risks and implements policies to reduce the likelihood of the potential for harm:

 When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing their own images on the Internet eg on social networking sites.
 Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. They are advised that they should not store pictures of pupils on school or personal devices but should copy them on to the School's network for storage.
 Care should be taken when taking digital / video images that pupils / pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute. Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.

Radicalisation and the Use of Social Media to encourage extremism

The internet and the use of social media in particular has become a major way to communicate with others, especially young people, which has provided access for like-minded people to create an online community and confirm extreme beliefs such as extreme ideological views or the use of violence to solve problems. This has led to social media becoming a platform for:

- intensifying and accelerating the radicalisation of young people;
- confirming extreme beliefs;
- accessing to likeminded people where they are not able to do this off-line, creating an online community;
- normalising abnormal views and behaviours, such as extreme ideological views or the use of violence to solve problems and address grievances.

Our school has a number of measures in place to help prevent the use of Social Media for this purpose:

- Web site filtering is in place to help prevent access to terrorist and extremist material and social networking sites such as Facebook, Instagram or Twitter by Pupils
- Pupils, Parents and Staff are educated in safe use of Social Media and the risks posed by on-line activity, including from extremist and terrorist groups.

Further details on how social media is used to promote extremism and radicalisation can be found in guidance from the Department for Education '*How Social Media Is Used to Encourage Travel to Syria And Iraq: Briefing Note For Schools.'*

Reporting of e-Safety issues and concerns including concerns regarding Radicalisation

Our school has clear reporting mechanisms in place, available for all users to report issues and concerns. For staff, any concerns regarding e-safety should be made to the e-safety officer who will review the issue and take the appropriate action. For pupils, they are taught to raise any concerns to their class teacher who will then pass this on to the e-safety officer. Complaints of a child protection nature must be dealt with in accordance with our child protection procedure.

Our Designated Safeguarding Lead provides advice and support to other members of staff on protecting children from the risk of on-line radicalisation. Oakmeadow ensures staff understand what radicalisation and extremism mean and why people may be vulnerable to being drawn into terrorism. We ensure staff have the knowledge and confidence to identify children at risk of being drawn into terrorism, and to challenge extremist ideas which can be used to legitimise terrorism. Staff safeguard and promote the welfare of children and know where and how to refer children and young people for further help as appropriate by making referrals as necessary to Channel.

Assessing Risks:

- We will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. The school cannot accept liability for any material accessed, or any consequences of Internet access.
- Emerging technologies, such as mobile phones with internet access (smartphones) are not governed by the school's infrastructure and bypass any and all security and filtering measures that are or could be deployed.

- We will audit ICT use to establish if the e-Safety policy is sufficiently robust and that the implementation of the e-safety policy is appropriate and effective.
- Methods to identify, assess and minimise risks will be reviewed regularly.
- Emerging technologies will be examined by the Head for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Any person not directly employed by the school will not be provided with access to any of the school systems with the exception of filtered Wi-Fi access.

Cyber-Bullying

Cyberbullying is bullying using technology to threaten, embarrass or cause discomfort. Seven categories of cyber-bullying have been identified:

- **Text message bullying** involves sending unwelcome texts
- **Picture/video-clip bullying via mobile phone cameras** with images or video clips usually sent to other people.
- **Phone call bullying via mobile phone** uses silent calls or abusive messages. Sometimes the bullied person's phone is stolen and used to harass others, who then think the phone owner is responsible.
- **Email bullying** often using a pseudonym for anonymity or using someone else's name to pin the blame on them.
- **Online grooming, Chat room and Social Networking Site abuse** involves sending menacing or upsetting responses to pupils or young people.
- **Bullying through instant messaging (IM)** is an Internet-based form of bullying where pupils and young people are sent unpleasant messages as they conduct real-time conversations online;
- **Bullying via websites** includes the use of defamatory blogs (web logs), personal websites and online personal polling sites. There has also been a significant increase in social networking sites for young people, which can provide new opportunities for cyber-bullying

ICT based sexual abuse

The impact on a child of ICT based sexual abuse is similar to that for all sexually abused pupils. However, it has an additional dimension in that there is a visual record of the abuse. ICT based sexual abuse of a child constitutes significant harm through sexual and emotional abuse. Recognition and response is recognising a situation where a child is suffering, or is likely to suffer a degree of physical, sexual and/or emotional harm (through abuse or neglect) which is so harmful that there needs to be compulsory intervention by child protection agencies into the life of the child and their family. All adults (volunteers, staff) working with pupils, adults and families will be alerted to the possibility that:

- A child may already have been/is being abused and the images distributed on the internet or by mobile telephone;
- An adult or older child may be grooming a child for sexual abuse, including involvement in making abusive images. This process can involve the child being shown abusive images;
- An adult or older child may be viewing and downloading child sexual abuse images.

Chat Room Grooming and Offline Abuse

Our staff will need to be continually alert to any suspicious activity involving computers and the Internet. Grooming of pupils online is a faster process than usual grooming, and totally anonymous. The abuser develops a 'special' relationship with the child online (often adopting a false identity), which remains a secret to enable an offline meeting to occur in order for the abuser to harm the child.

Taking and Storing Images of children including Mobile Phones (See our related documents)

Oakmeadow provides an environment in which children, parents and staff are safe from images being recorded and inappropriately used in turn eliminating the following concerns.

- Staff being distracted from their work with children.
- The safeguarding of children from inappropriate use of mobile phone cameras and other digital recording equipment.

The school has a Mobile Phone Policy which includes:

- the commitment to keep the children safe;

- how we manage the use of mobile phones at Beech Lodge School taking into consideration staff, pupils on placement, volunteers, other professionals, trustees, visitors and parents/carers;
- how we inform parents/carers, visitors and other professional of our procedures;
- what type of mobile phones will be used on educational visits and learning outside the classroom;
- The consequences of any breaches of this policy;
- Reference to other policies, such as whistleblowing and safeguarding children policies.

Filtering

The school will work in partnership with the Local Authority (T&W which manages ICT at Oakmeadow).

School has a full curriculum to support developing pupil and staff understanding around the Prevent agenda.

Technical – Infrastructure / Equipment, Filtering and Monitoring

The school 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. It also ensures that the relevant people named in the Roles and Responsibilities sections are effective in carrying out their E-Safety responsibilities:

 School Servers are securely located and physical access is restricted.
 All users are provided with a username and password by the Network Manager who keeps an up to date record of users and their usernames. Users are required to change their password on a regular basis.
 School ICT technical staff may monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Policy.
 Actual / potential E-Safety incidents are reported immediately to the E-Safety Officer who will arrange for these to be dealt with immediately in communication with the Network Manager/DSL, reporting to the Head Master. Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations 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 anti-virus software. Advice is given to staff and pupils about ensuring they have password protection on mobile devices.

Video Conferencing

- IP videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet.
- Pupils should ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing will be appropriately supervised for the pupils' age.

Managing Emerging Technologies Including Mobile Phones (reference to the mobile phone policy and the child protection policy in regard to the se of phones in school)

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones will not be used during school day.
- The sending of abusive or inappropriate text messages is forbidden.

Published Content and the School Web Site

- The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- The headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing Pupils' Images and Work

- The School will gain parental permission before using photographs of children or their work on the school's website, or in newsletters and other publications.
- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Pupils' names will not be used anywhere on the Web site or Blog in association with photographs.
- There is a statement in the school prospectus referring to our policy on digital images of children.

Information System Security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- Security strategies will be discussed with the Local Authority.

Protecting Personal Data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

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.

Staff Must Ensure that they:

 Acknowledge their acceptance of the Acceptable Use Policy.

 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 <u>that they are properly "logged-off" at the end of any session in which they are using personal data.</u>

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Shropshire Council can accept liability for the material accessed, or any consequences of Internet access.
- The school should audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.

Handling e-safety Complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures. (Please seek guidance in the safeguarding policy)
- Parents wishing to complain about e-safety issues should use the established school complaints procedure.
- Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

Communication of Policy (please also refer to the school's social media policy)

Pupils

- **Rules for Internet access will be made clear by all members of staff in charge of pupils learning.**
- **Pupils will be informed that Internet use will be monitored.**

Staff

- **All staff will be informed about and given access to the School e-Safety Policy and its importance explained.**
- **Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.**

Parents

- **Parents' attention will be drawn to the School e-Safety Policy and social media use policy in newsletters, the school prospectus and on the school Web site.**

Communications

A wide range of rapidly developing communications technologies have the potential to enhance learning. 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 need to be aware that email communications may be monitored.***

- ***Users must immediately report the receipt of any email that makes them feel uncomfortable, is offensive, threatening, extreme or bullying in nature and must not respond to any such email.***

- ***Any digital communication between staff and pupils or parents / carers (email, chat, VLE etc) must be professional in tone and content.***

- ***Pupils should be taught about email safety issues, such as the risks attached to the use of personal details.***

Responding to Incidents of Misuse:

It is hoped that all members of the school community will be responsible users of ICT, 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. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If any apparent or actual misuse appears to involve illegal activity, such as:

- ***Child sexual abuse images.***

- ***Adult material which potentially breaches the Obscene Publications Act.***

- ***Criminally racist material.***

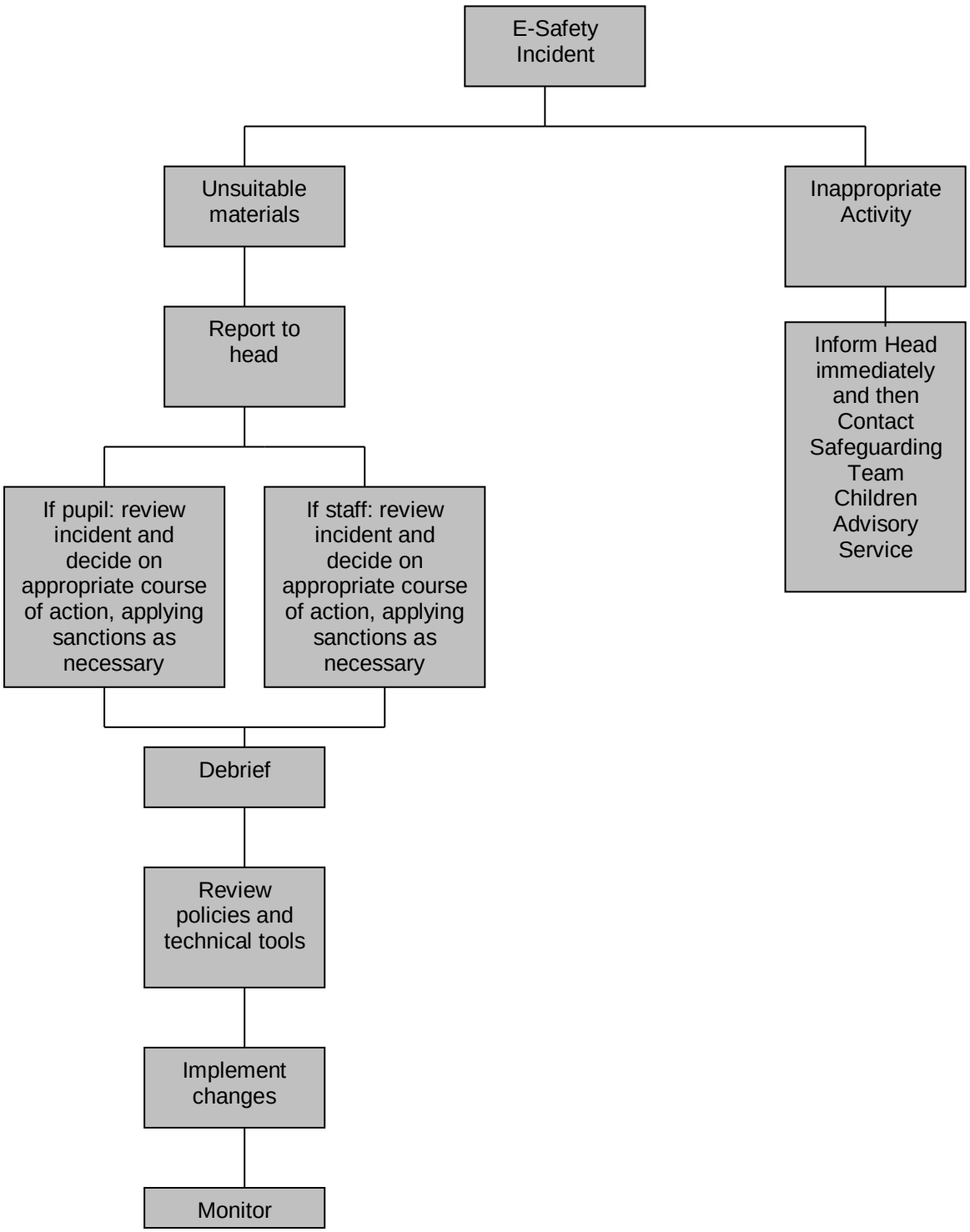
- ***Other criminal conduct, activity or materials.***

- ***Radicalisation***

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. However, if any illegal misuse is detected or reported action will be taken in accordance with the Acceptable Use policy and disciplinary action may be taken.

Appendix A

Flowchart for responding to e-safety incidents in school



Adapted from Becta – E-safety 2005

Amended and updated –Summer 2017- ratified

Appendix B

Key Stage 2

Think then Click

e-Safety Rules for Key Stage 2

- We ask permission before using the Internet.
- We only use websites that an adult has chosen.
- We tell an adult if we see anything we are uncomfortable with.
- We immediately close any webpage we not sure about.
- We only e-mail people an adult has approved.
- We send e-mails that are polite and friendly.
- We never give out personal information or passwords.
- We never arrange to meet anyone we don't know.
- We do not open e-mails sent by anyone we don't know.
- We do not use Internet chat rooms.

e-Safety Rules

These e-Safety Rules help to protect pupils and the school by describing acceptable and unacceptable computer use.

- The school owns the computer network and can set rules for its use.
- It is a criminal offence to use a computer or network for a purpose not permitted by the school.
- Irresponsible use may result in the loss of network or Internet access.
- Network access must be made via the user's authorised account and password, which must not be given to any other person.
- All network and Internet use must be appropriate to education.
- Copyright and intellectual property rights must be respected.
- Messages shall be written carefully and politely, particularly as email could be forwarded to unintended readers.
- Anonymous messages and chain letters are not permitted.
- Users must take care not to reveal personal information through email, personal publishing, blogs or messaging.
- The school ICT systems may not be used for private purposes, unless the headteacher has given specific permission.
- Use for personal financial gain, gambling, political activity, advertising or illegal purposes is not permitted.

The school may exercise its right to monitor the use of the school's computer systems, including access to web-sites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

Appendix C

Staff Information Systems Code of Conduct

To ensure that staff are fully aware of their professional responsibilities when using information systems, they are asked to sign this code of conduct. Staff should consult the school's e-safety policy for further information and clarification.

- The information systems are school property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.
- I will ensure that my information systems use will always be compatible with my professional rôle.
- I understand that school information systems may not be used for private purposes, without specific permission from the headteacher.
- I understand that the school may monitor my information systems and Internet use to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an appropriate system manager.
- I will not install any software or hardware without permission.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the school e-Safety Coordinator or the Designated Child Protection Coordinator.
- I will ensure that any electronic communications with pupils are compatible with my professional role.
- I will promote e-safety with pupils in my care and will help them to develop a responsible attitude to system use and to the content they access or create.

The school may exercise its right to monitor the use of the school's information systems, including Internet access, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

Signed:_____.

Print Name:_____.

Date:_____.

Amended and updated –Summer 2017- ratified