Scope of the Policy

This policy applies to all members of the school community (including staff, children / young people, volunteers, parents / carers, visitors) who have access to and are users of school ICT systems, both in and out of the school

Headteacher / Principal and Senior Leaders:

- The SMT has a duty of care for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the E-Safety Co-ordinator and class teachers.
- The SMT and e-safety co-ordinator should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. (see flow chart in later pages)
- The SMT is responsible for ensuring that the E-Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The SMT will receive regular monitoring reports from the E-Safety Co-ordinator as and when events arise.

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 and supports staff as the log and monitor e-safely concerns
- provides training and advice for staff;
- liaises with the Education Authority / relevant body;
- liaises with school technical staff;
- receives termly reports of e-safety incidents and creates a log of incidents to inform future e-safety developments;
- attends relevant meetings of pastoral care team and/or senior leadership team if required;
- reports regularly to Senior Leadership Team.

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 SMT, E-Safety Coordinator for investigation and action;
- all digital communications with children / 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;
- children understand and follow the e-safety and acceptable use policies;
- children have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- teachers 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 children should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.*

Child Protection Coordinator
should be trained in e-safety issues and be aware of the potential for serious child protection 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;
- Inappropriate sharing of images, for example through mobile phones.

Children:

- are responsible for using the school digital technology systems in accordance with the Acceptable Use Policy for children;
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so. They need to **un**derstand the need to protect themselves and respect others when participating in social networks;
- 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 work closely in partnership with parents on these issues through parents' evenings, newsletters, letters and social media. Parents and carers will be encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events;
- their children's personal devices in the school (where this is allowed).

Policy Statements

Education – children / young people
The e-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- a planned e-safety curriculum should be provided as part of all curricular areas when appropriate;
- children should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information;
- children should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet;
- children should be helped to understand the need for the Acceptable Use Agreement and be encouraged to adopt safe and responsible use both within and outside school;
- in lessons where internet use is pre-planned, it is best practice that children should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches;
- where children are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit;
- it is accepted that from time to time, for good educational reasons, students may need to research topics (for example racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Education & Training – Staff / Volunteers
It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- a planned programme of formal e-safety training will be made available to staff. This will be regularly updated. An audit of the e-safety personal learning needs of all staff will be carried out regularly. It is expected that some staff will identify e-safety as a professional learning need within the performance review and development process (PRD);
- all new staff should receive e-safety training as part of their induction programme, as identified in the induction booklet, ensuring that they fully understand the school e-safety policy, list of 'Do's and Don'ts and Acceptable Use Agreements;
- this E-Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days;
- the E-Safety Coordinator will provide advice / guidance / training to individuals as required.

Technical – infrastructure / equipment, filtering and monitoring

- school technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- there will be regular reviews and audits of the safety and security of school technical systems;
- servers, wireless systems and cabling must be securely located and physical access restricted;
- all users will have clearly defined access rights to school technical systems. Details of the access rights available to groups of users will be recorded by the Network Manager / Technical Staff (or other person) and will be reviewed, at least annually, by the E-Safety Committee (or other group);
- all users will be provided with a username and password by admin who will keep an up to date record of users and their usernames. Users will be required to change their password when instructed
- the "master / administrator" passwords for the school ICT system, used by the Network Manager must also be available to the Headteacher
  - SMT & Admin and technical admin are responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes
- the school has provided enhanced / differentiated user-level filtering through a filtering programme.
- school technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- an appropriate system to log e-safety issues is in place for users to report any actual / potential e-safety incident to the Class teacher, Network Manager / Technician
- appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software;
- an agreed policy is in place that allows staff to / forbids staff from installing programmes on school devices;

Use of digital and video images - Permission Form Available from School Office

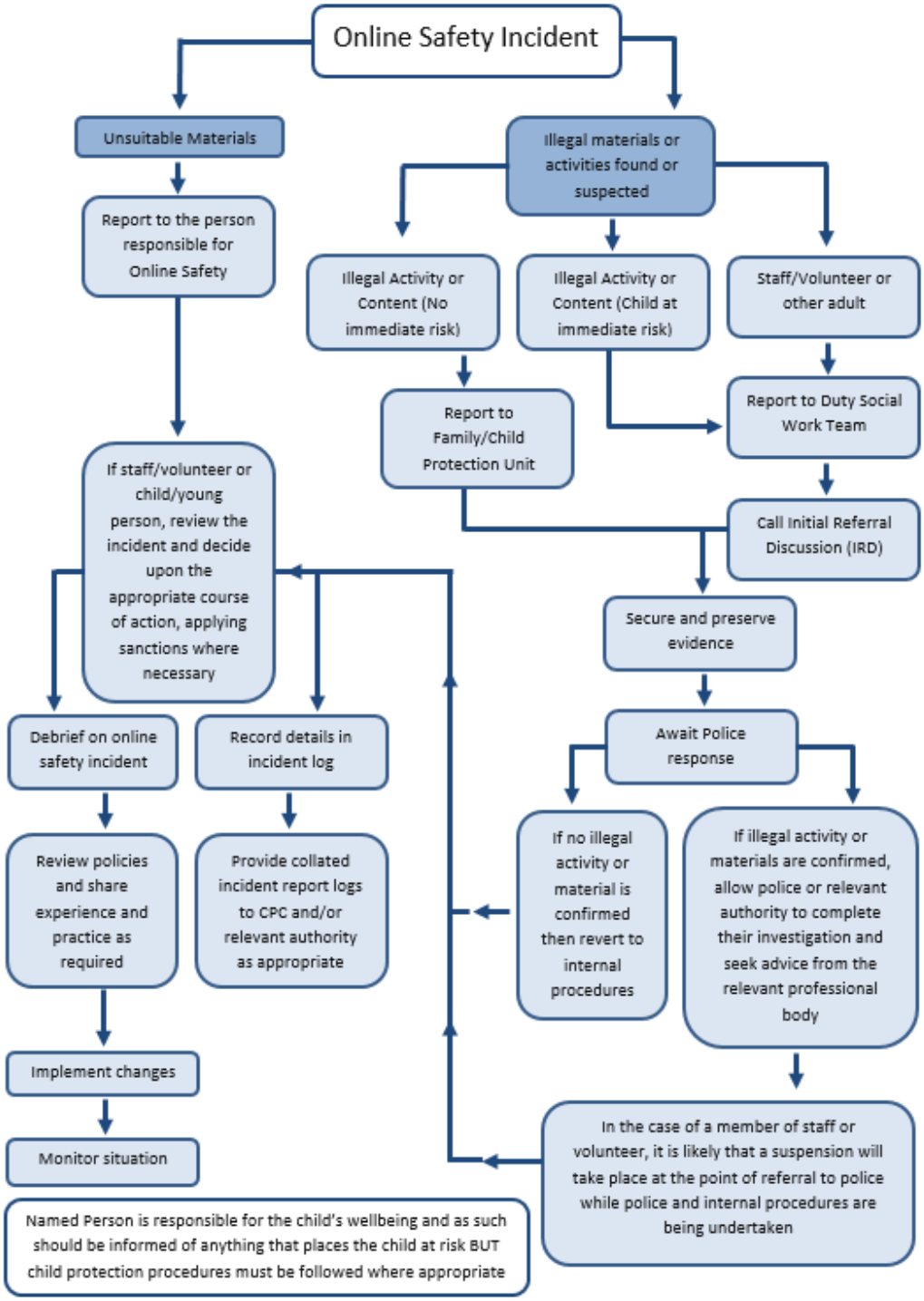
- when using digital images, staff should inform and educate children about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites, or sending inappropriate /intimate digital images which then may be shared further;
- Parents / carers are welcome to take videos and digital images of their children at school events for their own personal use. To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites (see social media policy)
- staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purpose unless approved by SMT;
- children must not take, use, share, publish or distribute images of others without their permission;
- photographs published on the school Facebook page, or elsewhere that include children will be selected carefully and will comply with good practice guidance on the use of such images;
- children's full names will not be used anywhere on a website or blog, particularly in association with photographs;
- written permission from parents or carers will be obtained at the start of the school year/ on enrolment
- learners' work can be published (a poem in a book for ex.) with the permission of the children and parents or carers.

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below) for responding to online safety incidents and report immediately to the police.



Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of concern all steps in this procedure should be followed:

- have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported;
- conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure;
- it is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection);
- record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below);
- once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following;
- internal response or discipline procedures;
- involvement by Local Authority or national / local organisation (as relevant);
- police involvement and/or action;
- **if content being reviewed includes images of Child Abuse then the monitoring should be halted and referred to the police immediately. Other instances to report to the police would include:**
    - incidents of 'grooming' behaviour;
    - the sending of obscene materials to a child;
    - adult material which potentially breaches the Obscene Publications Act;
    - criminally racist material;
    - other criminal conduct, activity or materials;
- **isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.**

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.