# E-safety Policy

**Key Information**

| | | |
|---|---|---|
| **Title** | E Safety Policy | |
| Prepared By | Mr McDermott | 22.12.17 |
| Checked By | Mrs Corrigan | |
| Approved By | Christian Vision Committee | |
| Version | V1 | |
| Document Update | Date 00.00.00 (Date of next review/update) | |

**Version History**

| **Version** | **Date** | **Amendments** |
|---|---|---|
| V01.0 | 23.01.18 | Amendments made to titles throughout – E-safety Co-Ordinator changed to Head of ICT<br>Changes to responsibility for cyber bullying |
| V01.1 | 00.00.00 | |
| V01.2 | 00.00.00 | |

January 2018

## Schedule for Review

| | |
|---|---|
| This E-safety policy was approved by the Governors on: | 23.1.18 |
| The implementation of this E-safety policy will be monitored by the: | E-safety Leader, Senior Leadership Team and SLICT |
| Monitoring will take place at regular intervals: | Annually |
| The Governors will receive a report on the implementation of the E-safety policy generated by the monitoring group (which will include anonymous details of E-safety incidents) at regular intervals: | Annually |
| 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. The next anticipated review date will be: | January 2019 |
| Should serious E-safety incidents take place the following external persons / agencies should be informed: | LA ICT Manager, LA Safeguarding Officer, Police |

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited)
- Internal monitoring data for network activity
- Surveys / questionnaires of:
  - students
  - parents and carers
  - staff

## Scope of the Policy

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

The Education and Inspections Act 2006 empowers the Headteacher, to such extent as is reasonable, to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other E-safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour for Excellence Policy.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate E-safety behaviour that take place out of school.

## Roles and Responsibilities

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 Governor. The role of the ICT Governor will include:

- regular meetings with the Head of ICT
- regular monitoring of E-safety incident logs
- regular monitoring of filtering logs
- reporting to relevant Governors meeting

**Headmistress and Senior Leaders**

- The Headmistress 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 Head of ICT, Director of Pastoral Care and Heads of Year.
- The Headmistress, Director of Pastoral Care and Director of Teaching and Learning are 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 on dealing with E-safety incidents included in a later section, "Responding to incidents of misuse" and relevant Local Authority HR).
- The Headmistress and Senior Leaders are responsible for ensuring that the Head of ICT 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 Headmistress and Senior Leaders 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.
- The Senior Leadership Team will receive regular monitoring reports from the Head of ICT.

**Head of ICT:**

- reports to SLICT;
- takes day to day responsibility for E-safety issues and has a leading role in establishing and reviewing the school E-safety policies and 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 the E-safety Governor to discuss current issues, review incident logs and filtering / change control logs;
- attends relevant meeting of Governors;
- reports regularly to the Senior Leadership Team.

**Network Manager**

The Network Manager is responsible for ensuring:

- 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 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;
- the filtering policy, is applied and updated on a regular basis and that its 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, remote access, email are regularly monitored in order that any misuse or attempted misuse can be reported to the Headmistress / Head of ICT for action;
- that monitoring software are implemented and updated as agreed in school policies.

**Teaching and Support Staff:**

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 (AUP)
- they report any suspected misuse or problems to the Headmistress, Director of Pastoral Care or Head of ICT for action;
- all digital communications with students, parents and/or 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;
- students understand and follow the E-safety and acceptable use policies;
- students have a good understanding of research skills and the need to avoid plagiarism 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 students 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:**

The DSL should be trained in E-safety issues and be aware of the potential for serious child protection and safeguarding issues to arise from:

- sharing of personal data;
- access to illegal and/or inappropriate materials;
- inappropriate on-line contact with adults / strangers;
- potential or actual incidents of grooming;
- cyber-bullying;
- Sexting.

**Students:**

- are responsible for using the school digital technology systems in accordance with the Student Acceptable Use Policy;

- 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;
- 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 and 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 and Carers**

Parents and Carers play a crucial role in ensuring that their children understand the need to use the internet and 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 and local E-safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good E-safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events;
- access to parents' sections of the website and on-line student records;
- their children's personal devices in the school (where this is allowed).

## Policy Statements

**Education – students**

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in E-safety is therefore an essential part of the school's E-safety provision. Children and young people need the help and support of the school to recognise and avoid E-safety risks and build their resilience.

E-safety should be a focus in all areas of the curriculum and staff should reinforce E-safety messages across the curriculum. The E-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned E-safety curriculum should be provided as part of ICT / Computing / PHSE / other lessons and should be regularly revisited .
- Key E-safety messages should be reinforced as part of a planned programme of assemblies and tutorial activities.
- Students 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.
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Students should be helped to understand the need for the student Acceptable Use Policy and encouraged to adopt safe and responsible use both within and outside school.
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices.
- In lessons, where internet use is pre-planned, it is best practice that students should be guided to sites checked as suitable for their use and that any unsuitable material that is found in internet searches should be reported to the Network manager / Head of ICT.
- Where students are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Network Manager can temporarily remove

those sites from the filtered list for the period of study. Any request to do so should be agreed with the Head of ICT in advance, with clear reasons for the need.

**Education – parents / carers**

Many parents and carers have only a limited understanding of E-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, website
- Parents / Carers evenings
- High profile events / campaigns, eg Safer Internet Day
- Reference to the relevant web sites / publications eg www.swgfl.org.uk www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers

**Education & Training – Staff / Volunteers**

It is essential that all staff receive E-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal E-safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the E-safety training needs of all staff will be carried out regularly.
- All new staff should receive E-safety training as part of their induction programme, ensuring that they fully understand the school E-safety policy and Acceptable Use Agreements.
- The Head of ICT will receive regular updates through attendance at external training events (eg from SWGfL / LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- This E-safety policy and its updates will be presented to and discussed by staff in staff meetings / INSET days.
- The Head of ICT (or other nominated person) will provide advice, guidance and training to individuals as required.

**Training – Governors**

Governors should take part in E-safety training and awareness sessions, with particular importance for those who are members of any subcommittee involved in technology, E-safety, health and safety and child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority, National Governors Association or other relevant organisation (eg SWGfL).
- Participation in school training and information sessions for staff or parents

**Technical – infrastructure / equipment, filtering and monitoring**

The school will be responsible for ensuring that the school network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their E-safety responsibilities:

- 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 and devices.
- All users will be provided with a username and secure password by *the Network Manager who will keep an up to date record of users and their usernames.* Users are responsible for the security of their username and password *and will be required to change their password every four weeks.*
- The " administrator" passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the Headmistress or other nominated senior leader and kept in a secure place.
- The Network Manager is 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.
- The school has provided differentiated user-level filtering (allowing different filtering levels for different groups of users, ie staff, students, etc).
- 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 Policy.
- An appropriate system is in place for users to report any actual or potential technical incident or security breach to the Network Manager or Head of ICT.
- 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 for the provision of temporary access of "guests" (eg trainee teachers, supply teachers, visitors) onto the school systems.

## Bring Your Own Device (BYOD)

The educational opportunities offered by mobile technologies are being expanded as a wide range of devices, software and online services become available for teaching and learning, within and beyond the classroom. This has led to the exploration by schools of users bringing their own technologies in order to provide a greater freedom of choice and usability. However, there are a number of E-safety considerations for BYOD that need to be reviewed prior to implementing such a policy. Use of BYOD should not introduce vulnerabilities into existing secure environments. Considerations will need to include levels of secure access, filtering, data protection, storage and transfer of data, mobile device management systems, training, support, acceptable use, auditing and monitoring. This list is not exhaustive and a BYOD policy should be in place and reference made within all relevant policies.

- The school has a set of clear expectations and responsibilities for all users.
- The school adheres to the Data Protection Act principles.
- All users are provided with and accept the Acceptable Use Agreement.
- All network systems are secure and access for users is differentiated.
- Where possible these devices will be covered by the school's normal filtering systems, while being used on the premises.
- All users will use their username and password and keep this safe.
- Mandatory training is undertaken for all staff.
- Students receive training and guidance on the use of personal devices.
- Regular audits and monitoring of usage will take place to ensure compliance.
- Any device loss, theft, change of ownership of the device will be reported as in the BYOD policy.
- Any user leaving the school will follow the process outlined within the BYOD policy.

**Use of digital and video images**

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents, carers and students need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate students 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.
- In accordance with guidance from the Information Commissioner's Office, parents and carers may take videos and digital images of their own children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published or made publicly available on social networking sites, nor should parents or carers comment on any activities involving other students in the digital / video images or take photographs of other students.
- 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 purposes
- Care should be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere, that include students will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' 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 before photographs of students are published on the school website - covered as part of the AUP signed by parents or carers at the start of the year
- Student's work can only be published with the permission of the student and parents or carers.

## Data Protection

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

**Communications**

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

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

* Use of school email for personal emails permitted for sixth form students only.

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 should be aware that email communications are monitored.
- Users must immediately report, to the nominated person and in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and students or parents / carers must be professional in tone and content.

**Social Media - Protecting Professional Identity**

All schools, academies and local authorities have a duty of care to provide a safe learning environment for students and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to students, staff and the school through limiting access to personal information:

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions.
- Risk assessment, including legal risk

School staff should ensure that:

- No reference should be made in social media to students, parents, carers or school staff.
- They do not engage in online discussion on personal matters relating to members of the school community.
- Personal opinions should not be attributed to the school or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

**Unsuitable / inappropriate activities**

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts usage as follows:

| User Actions | | Acceptable | Acceptable at certain times | Acceptable for nominated users | Unacceptable | Unacceptable and illegal |
|---|---|---|---|---|---|---|
| **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 –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978** | | | | | X |
| | **Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.** | | | | | X |
| | **Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character). Contrary to the Criminal Justice and Immigration Act 2008** | | | | | X |
| | **Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation). Contrary to the Public Order Act 1986** | | | | | X |
| | **Pornography** | | | | X | |
| | **Promotion of any kind of discrimination** | | | | X | |
| | **Threatening behaviour, including promotion of physical violence or mental harm** | | | | X | |
| | **Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute** | | | | X | |

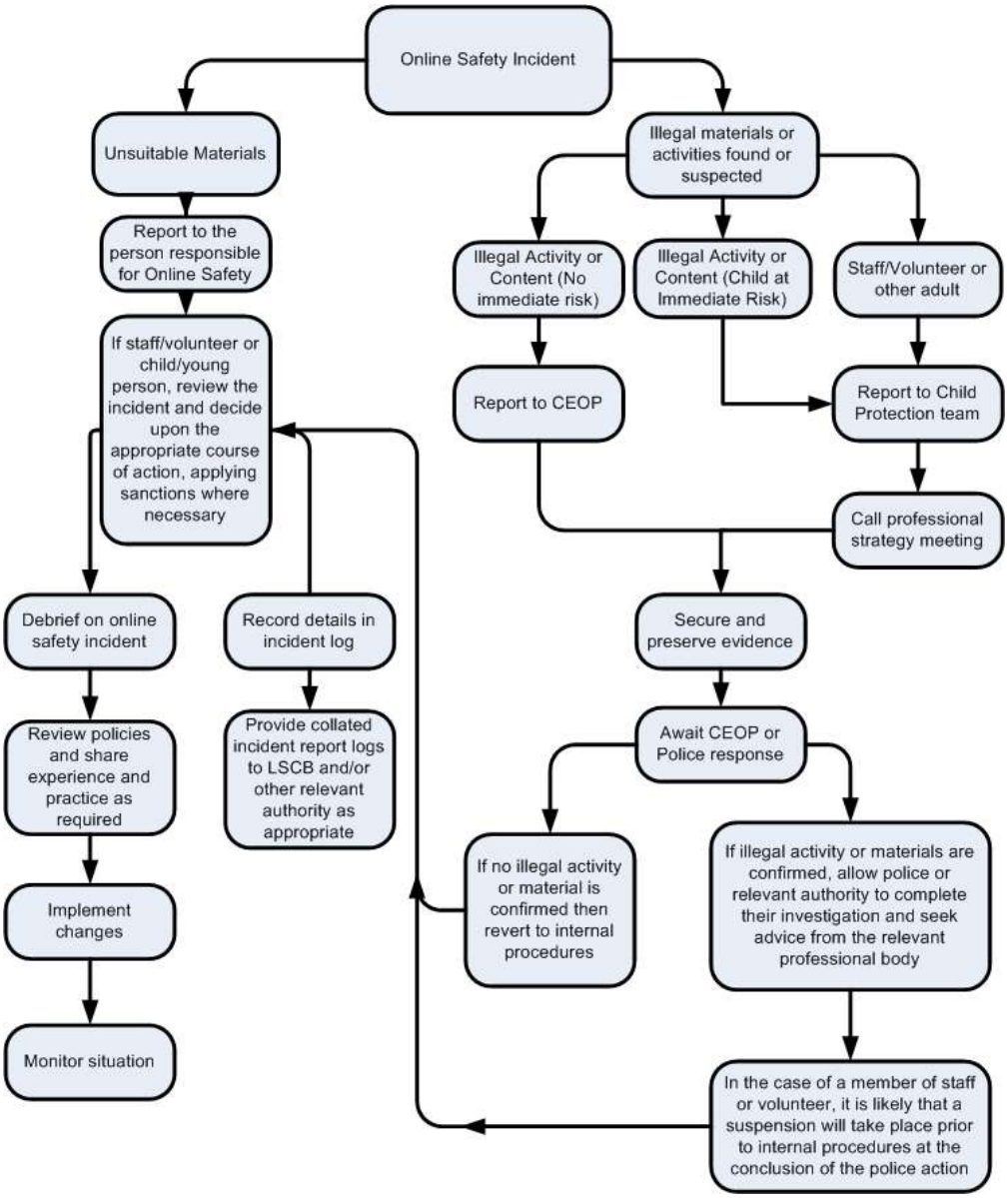
| User Actions | Acceptable | Acceptable at certain times | Acceptable for nominated users | Unacceptable | Unacceptable and illegal |
|---|---|---|---|---|---|
| **Using school systems to run a private business** | | | | X | |
| **Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy** | | | | X | |
| **Infringing copyright** | | | | X | |
| **Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)** | | | | X | |
| **Creating or propagating computer viruses or other harmful files** | | | | X | |
| **Unfair usage (downloading / uploading large files that hinders others in their use of the internet)** | | | | X | |
| **Online gaming (educational)** | | X | | | |
| **Online gaming (non-educational)** | | | | X | |
| **Online gambling** | | | | X | |
| **Online shopping / commerce** | | | | X | |
| **File sharing** | | | X | | |
| **Use of social media** | | | X | | |
| **Use of messaging apps** | | | X | | |
| **Use of video broadcasting, eg Youtube** | | | X | | |

**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 (see "User Actions" above).

**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 for responding to online safety incidents and report immediately to the police.


Online Safety Incident
Unsuitable Materials
Illegal materials or activities found or suspected
Report to the person responsible for Online Safety
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Debrief on online safety incident
Record details in incident log
Secure and preserve evidence
Review policies and share experience and practice as required
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Await CEOP or Police response
Implement changes
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
Monitor situation
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action

**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 suspicion, 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.

**School Actions & Sanctions**

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as outlined in the Behaviour for Excellence Policy.

To be read in conjunction with the following policies;

- Behaviour for Excellence Policy
- Acceptable Use Policy (Student and Staff)
- Anti-Bullying Policy
- Equalities Objectives
- SMSC Policy
- Staff Code of Conduct
- Safeguarding and Child Protection Policy