# English Martyrs' Catholic Voluntary Academy

# Online Safety, Online Learning and Adult Acceptable Use Policy

Our School Mission Statement

Love one another

Inspire and respect

Grow in friendship

Have faith

Trust in God

DRAFT

Date : Review Date:

## School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools / academies and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times, as many new technologies can also present dangers for users.

## This Policy is intended to ensure that:

- Young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- School systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- Parents and carers are aware of the importance of e-safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

## Contents

This document will be split up into the following sections:

| Schedule for Development / Monitoring / Reviews | |
|---|---|
| This online safety policy was approved in principle by the full Governing Body on: | |
| The implementation of this online safety policy will be monitored by the: | **Computing Leader: E. Pugh, E. Jepson**<br>**Designated Safeguard Lead: K. Mann** |
| Monitoring will take place at six monthly intervals: | |
| On request, the Governing Body can receive a report on the implementation of the e-safety policy generated by the SLT and Computing leader (which will include anonymous details of online safety incidents). | **The next anticipated review date will be:**<br>**November 2017** |
| The Online 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:**<br>**November 2017** |
| Should serious e-safety incidents take place, the following persons should be informed: | **K. Mann**<br>**H. McElhone** |

DRAFT

## Scope of the Policy

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

The Education and Inspections Act 2006 empowers Head teachers to such an extent as is reasonable to regulate the behaviours of students when they are off school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other online 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 Policy.

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

**Education - Pupils**

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

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

- A planned online safety curriculum should be provided as part of the computing lessons and should be regularly revisited
- Key messages should be reinforced with particular attention to SMART
- Pupils should be taught in all lessons to be critically aware of the materials and content they access online and be guided to validate the accuracy of information
- Pupils should be taught to acknowledge the source of information used
- Pupils should be helped to understand the need for the pupil Acceptable Use Policy and encouraged to adopt safe and responsible use within and outside the classroom
- 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

**Education – Parents/Carers**

Many parents and carers may have only limited understanding of online safety risks and issues, yet they play an essential role in the education of their child/ren and in the monitoring/regulation of the children's online behaviours. Parents may underestimate how often children 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:

- Parent forums
- Information shared on school website
- High profile events e.g. Safer Internet Day
- Reference to relevant websites

DRAFT

## Education & Training – Staff/Volunteers

It is essential that all staff receive online safety training and understand their responsibilities to protect pupils from harm from online safety incidents. Training will be offered as follows:

- Training through staff meetings delivered by CEOP Ambassador – an audit of staff needs to be carried out annually and addressed through individual CPD opportunities
- All new staff will have an online safety induction
- All staff to sign and understand the Acceptable Use Agreements
- Staff to be directed to relevant sites for additional training such as CEOP and NSPCC
- The Online Safety Policy is up to date and shared with staff
- Staff receive annual Safeguarding training which includes online safety

## Governor Training

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

- Attendance at training provided by Local Authority, National Governors Association, Diocese or other relevant professional organisations
- Participation in school training or information sessions for staff and parents, this may include attendance at assemblies/lessons

DRAFT

# English Martyrs’ Catholic Voluntary Academy
## Online Safety - Staff Acceptable Use Agreement

**Acceptable Use Policy Agreement**
I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that students / pupils receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

| For my professional and personal safety |
|---|
| I understand that the school will monitor my use of the ICT systems, email and other digital communications. |
| I understand that the rules set out in this agreement also apply to the use of school ICT systems (e.g. laptops, email, VLE etc) out of school, and to the transfer of personal data (digital or paper based) out of school. |
| I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school. |
| I will not disclose my username or password to anyone else, nor will I try to use any other person’s username and password. I understand that I should not write down or store a password where it is possible that someone may steal it. |
| I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person. |
| I will not refer to students/pupils/parents/carers or school staff when using social media. |
| I will not engage in online discussion on personal matters relating to members of the school community. |
| I understand that personal opinions should not be attributed to the school and should not bring the school into disrepute. |
| I will regularly check security settings on personal social media profiles to minimise the loss of personal information. |
| All work related emails will be sent using the school email system. |
| I will be responsible for the security of my personal username and password and will be required to change the password every three months. |

DRAFT

| Professional communication |
|---|
| I will not access, copy, remove or otherwise alter any other user’s files, without their express permission. |
| I will communicate with others in a professional manner, I will not use aggressive or inappropriate language. I will appreciate that others may have different opinions. |
| I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school’s policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website) it will not be possible to identify by name, or other personal information, those who are featured. Photographs taken in school are the property of the school and should not be downloaded onto my own equipment without expression permission from the Headteacher and they should not be stored on my equipment. |
| I will never use chat and social networking on my own devices in working hours. |
| I will only communicate with students / pupils and parents / carers using official school systems and no forms of social media. Any such communication will be professional in tone and manner. |
| I will not engage in any on-line activity that may compromise my professional responsibilities or the good name of the school. |
| Users must immediately report, to the nominated persons, 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. |

| Bring your own device |
|---|
| Although strongly discouraged any devices brought from home will be password protected , encrypted and free from any inappropriate content – they must be checked and passed by RMG Systems |
| I will ensure that my devices are given to the network technician to ensure they use the school filtering system. |
| Any device loss, theft, change of ownership will be reported to the ICT Leader. |
| Ensure that you have made all the appropriate measures to keep your device virus-free (install virus-software, choose a secure operating system etc.) |

| When using the internet in my professional capacity |
|---|
| I will ensure that I have permission to use the original work of others in my own work. |
| Where work is protected by copyright, I will not download or distribute copies (including music, videos, software). |

DRAFT

| Safe use of technology |
|---|
| When I use my mobile devices (PDAs / laptops / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses. Chargers should be PAT tested. |
| 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 search. Online Safety pathways to be used to guide the children. |
| I will use school email addresses on the school ICT systems. In some cases my personal email will be used by agreement with the Headteacher. |
| I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted , or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes). |
| I will ensure that my data is regularly backed up, in accordance with relevant school policies – see computer disaster recovery plan. |
| I will not upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or any inappropriate material which may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials – if this happens or I inadvertently access inappropriate material then I will immediately report it to the network administrator and child protection officer. |
| will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings. I will not disable or cause any damage to school equipment, or the equipment belonging to others. |
| I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Data Protection Policy. Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage. |
| I understand that the data protection policy requires that any staff or student / pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by the school policy to disclose such information to an appropriate authority (freedom of information policy). |
| I will immediately report any damage or faults involving equipment or software, however this may have happened. |
| I will monitor use of digital technology, mobile devices, cameras etc in lessons and other school activities. |

DRAFT

| Use of digital and video imaging |
|---|
| When using digital images, staff should inform and educate students pupils about the risks associated with taking, using, sharing, publishing and distributing images. In particular, they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites. |
| In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their 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 / carers comment on any activities involving other students / pupils in the digital / video images. |
| 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. Images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes, unless express permission is given by the headteacher – in which case all images should be transferred to school equipment and removed from personal equipment. |
| Care should be taken when taking digital / video images that students / 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 students / pupils will be selected carefully and will comply with expectations of good practice in school. |
| Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs. |
| Pupil's work can only be published after discussion with the student and with their permission. |
| Students must not take, use, share, publish or distribute images of others without their permission. |

DRAFT

## Staff Online Safety Acceptable Use Policy Agreement

**I understand that I am responsible for my actions in and out of the school.**

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.

- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include being given a warning. The matter may be referred to the Governors at the school for a decision on disciplinary action, which may involve suspension or dismissal. The Local Authority may be involved, and in the event of illegal activities there will be the involvement of the police.

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name

Signed

Date

DRAFT

# English Martyrs' Catholic Voluntary Academy
## Technical Online Safety Policy

DRAFT

### Introduction

The school will be 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 will also need to ensure that relevant staff receive guidance and training and will be effective in carrying out their responsibilities:

Effective technical security depends not only on technical measures, but also on appropriate policies and procedures and on good user education and training. The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that:

- users can only access data to which they have right of access
- no user should be able to access another's files (other than that allowed for monitoring purposes within the school's policies).
- access to personal data is securely controlled in line with the school's personal data policy
- logs are maintained of access by users and of their actions while users of the system
- there is effective guidance and training for users
- there are regular reviews and audits of the safety and security of school systems.
- there is oversight from senior leaders and these have impact on policy and practice.

### Responsibilities

The management of technical security will be the responsibility of RMG Systems

| Technical Security |
|---|
| Appropriate security measures are in place to protect school systems from accidental or malicious attempts which may threaten the security of the school systems and data. |
| Servers, wireless systems are be securely located and physical access restricted. |
| RMG Systems are responsible for ensuring that software license 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. |
| All computers and devices in school should be locked down to keep them safe and should have access to the school's filtering systems. |
| Any potential threats to safety or security should be reported to a member of Senior Management immediately. |
| Records of all users and rights to be audited and kept by Mrs C Carty |
| 'Guest' users should be provided with separate login details (e.g. students). |
| The school infrastructure and individual workstations are protected by up to date software to protect against malicious attacks. |

| |
|---|
| Any filtering issues should be reported immediately to the filtering provider. |
| Changes to the filtering system should be checked and audited. |
| Any websites that have been accessed that included inappropriate content should be reported to SLT, logged and investigated |
| If staff bypass the filtering system by use of the password they must not permanently allow access to any sites. |

| **Password Security** |
|---|
| Where required all adults and KS2 children will be given their own username and password. |
| Passwords for new users, and replacement passwords for existing users will be allocated by RMG Systems and K.Mann. |
| All users have clearly defined access rights to school systems. |
| The administrator passwords for the school will be made available for technical staff, the headteacher and appointed senior leader. |
| Staff are encouraged to change their passwords every three months, or in the event of a breach of privacy. |
| Passwords should be different for different systems and must be secure. |
| Users must not allow othe users to access the system using their log on details and must immediately report any suspicion or evidence that there has been a breach of security. |

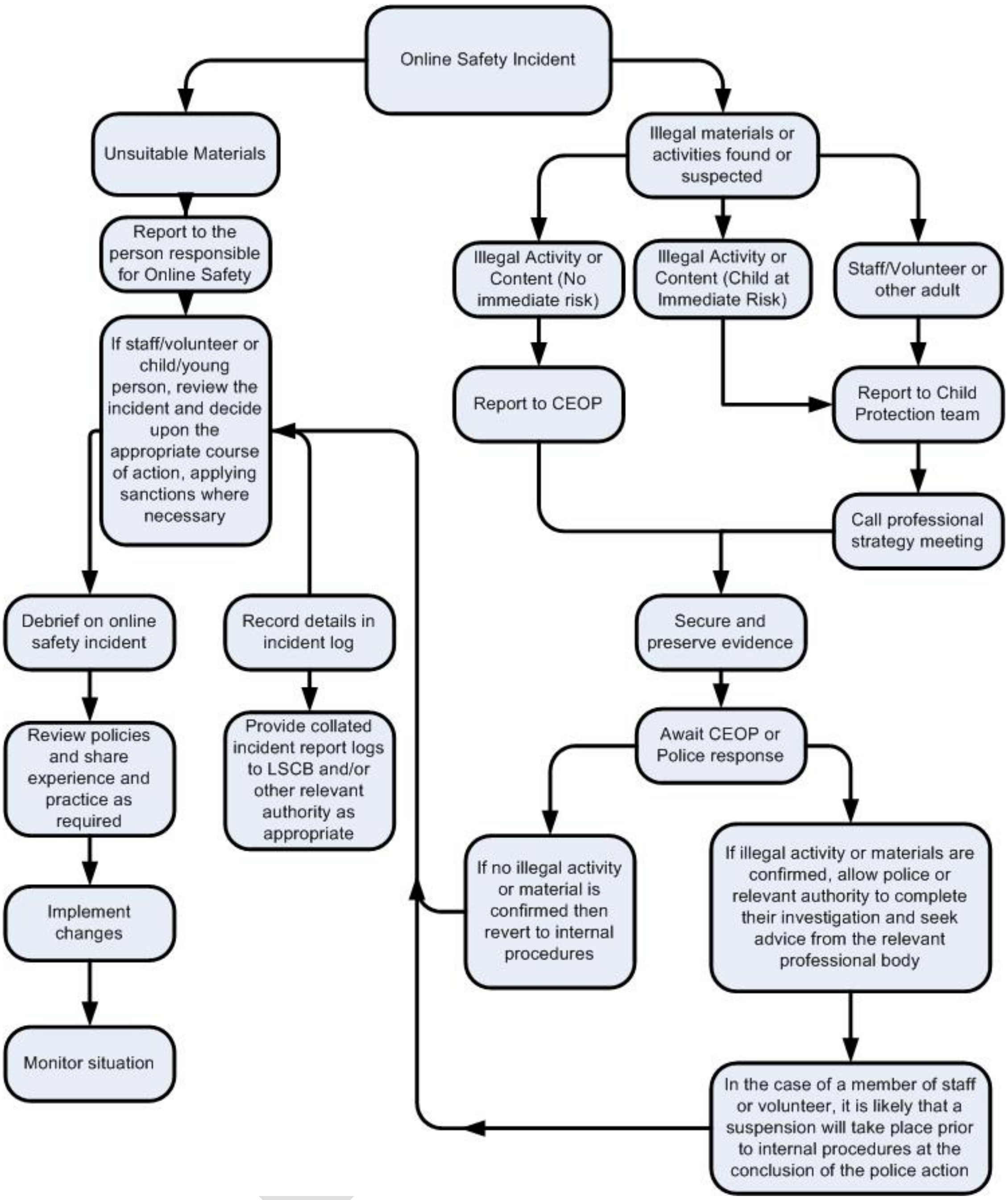
DRAFT

**Online Safety leader responsibilities:**

- 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 online safety incident taking place.
- Provides training and advice for staff
- Liaises with technicians
- Receives reports of online safety incidents and creates a log of incidents to inform future online safety developments,
- Meets regularly with Online Safety/Safeguarding Governor to discuss current issues, review incident logs and filtering / change control logs
- Attends relevant meetings and committee of Governors
- Reports regularly to the Headteacher and immediately of any breaches to online safety

DRAFT

Procedures for Dealing with Breach of Online Safety Incident


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
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
Implement changes
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

**In the event of suspicion, all steps in this procedure should be followed:**

- 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 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.

DRAFT

## User Actions

| | | Acceptable | Acceptable at certain times | Acceptable for nominated | 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** | | | | | |
| | **Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.** | | | | | |
| | **Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008** | | | | | |
| | **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** | | | | | |
| | **Pornography** | | | | | |
| | **Promotion of any kind of discrimination** | | | | | |
| | **Threatening behaviour, including promotion of physical violence or mental harm** | | | | | |
| | **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** | | | | | |
| **Using school systems to run a private business** | | | | | | |
| **Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy** | | | | | | |
| **Infringing copyright** | | | | | | |
| **Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)** | | | | | | |
| **Creating or propagating computer viruses or other harmful files** | | | | | | |
| **Unfair usage (downloading / uploading large files that hinders others in their use of the internet)** | | | | | | |
| **On-line gaming (educational)** | | | | | | |
| **On-line gaming (non-educational)** | | | | | | |
| **On-line gambling** | | | | | | |
| **On-line shopping / commerce** | | | | | | |
| **File sharing** | | | | | | |
| **Use of social media** | | | | | | |
| **Use of messaging apps** | | | | | | |
| **Use of video broadcasting e.g. Youtube** | | | | | | |

| Incident Checklist | Refer to class teacher | Refer to Computing Leaders | Refer to Headteacher | Refer to Police | Refer to technical support staff for action re filtering / security etc | Inform parents / carers | Removal of network / internet access rights | Warning | Further sanction e.g. detention or exclusion |
|---|---|---|---|---|---|---|---|---|---|
| Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities). | | | | | | | | | |
| Unauthorised use of non-educational sites during lessons | | | | | | | | | |
| Unauthorised use of mobile phone / digital camera / other mobile device | | | | | | | | | |
| Unauthorised use of social media / messaging apps / personal email | | | | | | | | | |
| Unauthorised downloading or uploading of files | | | | | | | | | |
| Allowing others to access school network by sharing username and passwords | | | | | | | | | |
| Attempting to access or accessing the school network, using another pupil’s account | | | | | | | | | |
| Attempting to access or accessing the school network, using the account of a member of staff | | | | | | | | | |
| Corrupting or destroying the data of other users | | | | | | | | | |
| Sending an email, text or twitter message that is regarded as offensive, harassment or of a bullying nature | | | | | | | | | |
| Continued infringements of the above, following previous warnings or sanctions | | | | | | | | | |
| Actions which could bring the school into disrepute or breach the integrity of the ethos of the school | | | | | | | | | |
| Using proxy sites or other means to subvert the school’s filtering system | | | | | | | | | |
| Accidentally accessing offensive or pornographic material and failing to report the incident | | | | | | | | | |
| Deliberately accessing or trying to access offensive or pornographic material | | | | | | | | | |
| Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act | | | | | | | | | |

Name: ________________________________

Date: ________________________________

Online Safety Lead: ________________________________

DRAFT

| Reporting Log<br>Group ............................................................ | | | | | | |
|---|---|---|---|---|---|---|
| Date | Time | Incident | Action taken | | Incident Reported by | Signature |
| | | | What? | By whom? | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

DRAFT