



Mount Carmel

R.C. HIGH SCHOOL



Online Safety Policy

Last review date: July 2025 – Mr R Foster

Next review date: July 2026 – Mr R Foster

A Family of Faith & Learning

Version control record since February 2020

Please note that where the policy is LCC model policy, then the version details will be provided by LCC in the document.

Schedule for development, monitoring and review of this policy

| | |
|---|--|
| This online safety policy was approved by the <i>Governing Body</i> on: | September 2024 |
| The implementation of this online safety policy will be monitored by the: | DSL Team |
| Monitoring will take place at regular intervals: | Annually |
| The <i>Governing Body</i> will receive an update containing online safety incidents at regular intervals: | At Governor ECM committee meetings |
| 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 online safety or incidents that have taken place. The next anticipated review date will be: | Summer Term 2025 |
| Should serious online safety incidents take place, the following persons should be informed: | Mr J Hill (DSL) Mr D Sweeney (Back-up DSL) Mr R Foster (Back-up DSL) |

The school will monitor the impact of the policy using:

- *Logs of reported incidents held within CPOMS*
- *Smoothwall system*
- *Surveys / questionnaires of*
 - *students / pupils*
 - *parents / carers*
 - *staff*

Scope of the Policy

This policy applies to all members of the *school* (including staff, students / pupils, volunteers, parents / carers, visitors, guests) 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 Headteachers to such extent as is reasonable, to regulate the behaviour of pupils 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 cyberbullying, 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 school's Behaviour 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 online safety behaviour that take place out of school.

Roles and Responsibilities

Governors

Governors are responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy. This will be carried out by the governors receiving regular information about online safety incidents and monitoring reports. A member of the governing body (P Holden) has taken on the role of online safety governor. The role of the online safety governor will include:

- regular meetings with the online safety coordinator (~~R Foster~~) and the DSL team (~~J Hill~~).
- regular monitoring of online safety incident logs through CPOMS/ Smoothwall.
- regular monitoring of filtering / change control logs in liaison with ~~L Robinson~~ the Network Manager
- reporting to governors

Headteacher and Senior Leaders

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community
- The Headteacher should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The Headteacher is responsible for ensuring that the online safety coordinator and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Headteacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and support to those colleagues who take on important monitoring roles.

The Online Safety Co-ordinators Designated Safeguarding Leads

- lead the online safety working party
- take day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents
- ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provide training and advice for staff
- liaise with the Local Authority / relevant body
- liaise with school technical staff
- receive reports of online safety incidents and creates a log of incidents to inform future online safety developments,
- meet regularly with the online safety governor to discuss current issues, review incident logs and filtering / change control logs
- attend relevant meeting / committee of governors
- report regularly to SLT

should be trained in online safety issues and be aware of the potential for serious child protection / safeguarding 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

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 online safety technical requirements and any Local Authority / other relevant body online safety policy / guidance that may apply.
- that users may only access the networks and devices through properly enforced password protection

- 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 online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the network / internet / email may be monitored in order that any misuse / attempted misuse can be reported to the online safety coordinator / DSL team

All Staff

are responsible for ensuring that:

- they have an up-to-date awareness of online safety matters and of the current school online safety policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy (AUP) and Digital Communications Policy
- they report any suspected misuse or problem to the online safety coordinator / Headteacher for investigation / action / sanction
- all digital communications with students / parents / carers should be on a professional level and only carried out using official school systems
- online safety issues are embedded in all aspects of the curriculum and other activities
- students understand and follow the online 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 pupils 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

Pupils

are responsible for using the school digital technology systems in accordance with the Student Acceptable Use Policy (E-safety Policy). This can be found on the school website.

- 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 / use of images and on cyber-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's online 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 help parents understand these issues through parents' evenings, newsletters, letters, website and information about national / local online safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events

Guest Users

Guest users (e.g. supply teachers and visitors) may be given limited access to the school system and must follow the regulations outlined here as per the staff usage.

Policy Statements

Education - Pupils

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 online safety is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their 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:

- An online safety curriculum is provided as part of PSHCE/assemblies/computing
- Key online safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities
- Students should be taught in all lessons to be critically aware of the materials / content they access online 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 pupil Acceptable Use Agreement in the planner and encouraged to adopt safe and responsible use both within and outside school
- Students will be encouraged to report on other students who are putting themselves at risk by their online behaviour
- 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 pupils 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. These processes should include closing offensive content and reporting the incident to the Network Manager via the class teacher.
- Where pupils 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 (e.g. racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff should liaise with the network manager to see if sites can be temporarily removed from the filtered list for the period of study. Any request to do so should be auditable, with clear reasons for the need.

Education – Parents / Carers

Many parents and carers have only a limited understanding of online 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 online 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 / sessions
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications

Education and Training – Staff & Volunteers

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

- A programme of online safety training will be made available to staff through development time as part of the Hays safeguarding training. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly. Some staff may identify online safety as a training need within the appraisal process.
- All new staff will receive online safety training as part of their induction programme, ensuring that they fully understand the school Online Safety Policy and Acceptable Use Agreements.
- The online safety coordinator will receive regular updates through attendance at external training events (e.g. from LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- This online safety policy and its updates will be presented to and discussed by staff in staff meetings / INSET days / development time.
- The online safety coordinator will provide advice / guidance / training to individuals as required.

Training – Governors

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

- Attendance at training provided by the Local Authority / National Governors Association / or another relevant organisation
- Participation in school training as part of the Hays safeguarding package / information sessions for staff

Technical – infrastructure / equipment, filtering and monitoring

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 the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- The safety and security of school technical systems are reviewed regularly based on technological updates
- 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.
- The Headteacher is responsible for ensuring that software licence requirements are correctly satisfied considering the software and hardware in use 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 and monitored through the Smoothwall software
- School staff monitor the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement
- Any actual / potential technical incident / security breach should be reported immediately to the network manager
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems workstations, mobile devices etc. 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 virus software.

- Personal data must not be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Bring Your Own Device (BYOD)

At the moment, the school only allows staff members to access the school network through their own devices via a personalised password on to the school Wi-Fi. 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.

- 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 personal Wi-Fi username and password and keep this safe
- Mandatory training is undertaken for all staff
- Pupils are not allowed to use personal devices on the school network
- Regular audits and monitoring of usage will take place to ensure compliance

Use of digital and video images

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, parents / carers and pupils 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 pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites. This will be done through PSHCE and assemblies
- 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 in accordance with the school's safeguarding policy
- 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.
- Pupils must not take, use, share, publish or distribute images of others without their permission

- 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.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Permission from parents or carers will be obtained before photographs of students / pupils are published on the school website
- Pupil's work can only be published with the permission of the pupil and parents or carers.

Data Protection and GDPR

Personal data will be recorded, processed, transferred and made available according to the GDPR 2018, which highlights 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.

The school must ensure that:

- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a plan for reporting, logging, managing and recovering from information risk incidents as outlined as part of the school GDPR procedure
- There are clear policies about the use of cloud storage / cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner's Office.

Staff must ensure that they:

- 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 that they are properly "logged off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

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:

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

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. Staff and students should therefore use only the school email service to communicate with others when in school, or on school systems
- Users must immediately report to the online safety coordinator – 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 / pupils or parents / carers (email) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Whole class / group email addresses may be used
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

All schools 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 pupils, 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 pupils, 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.

The *school's* use of social media for professional purposes will be checked regularly by the online safety working party to ensure compliance with the online safety policy.

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:

| | | Acceptable | Acceptable at certain times | Acceptable for nominated users | Unacceptable | Unacceptable and illegal |
|---|--|------------|-----------------------------|--------------------------------|--------------|--------------------------|
| User Actions | | | | | | |
| 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 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 / pornographic material | | | | X | |
| | promotion of any kind of illegal discrimination | | | | X | |
| | Any form of illegal 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 | |
| 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 (e.g. financial / personal information, databases, computer / network access codes and passwords) | | | | | X | |

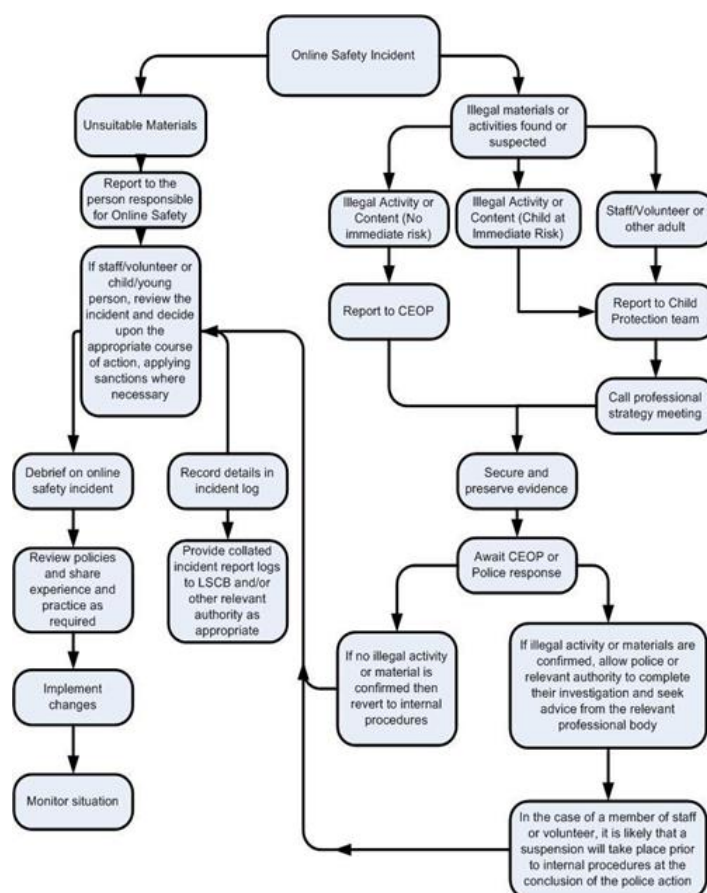
| | | | | | |
|---|--|---|--|---|--|
| Creating or propagating computer viruses or other harmful files | | | | X | |
| Unfair usage (downloading / uploading large files that hinders others in their use of the internet) | | | | X | |
| On-line gaming (educational) | | X | | | |
| On-line gaming (non-educational) | | X | | | |
| On-line gambling | | | | X | |
| On-line shopping / commerce | | X | | | |
| File sharing | | X | | | |
| Use of social media | | X | | | |
| Use of messaging apps | | X | | | |
| Use of video broadcasting e.g. 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 (below and appendix) 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 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.

School actions and consequences

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. Illegal activities will be reported to the relevant external agencies, as with inappropriate misuse where this is considered appropriate. Appropriate members of the school community will be made aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:

| Students / Pupils | | | | | | | | |
|---|------------------------|-------------------------------------|-----------------|--|-------------------------|---|---------|------------------|
| Incidents: | Refer to class teacher | Refer to inline safety co-ordinator | 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 |
| Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities). | | X | X | | | | | X |
| Unauthorised use of non-educational sites during lessons | X | | | | | | X | |
| Unauthorised use of mobile phone / digital camera / camera / another mobile device | X | X | | | X | | X | |
| Unauthorised use of social media / messaging apps / personal email | X | | | | X | | X | |
| Unauthorised downloading or uploading of files | X | | | X | | | | |
| Allowing others to access school network by sharing username and passwords | X | | | | | | X | |
| Attempting to access or accessing the school network, using another student's account | X | | | | | | X | |
| Attempting to access or accessing the school network, using the account of a member of staff | | X | | | X | | | X |
| Corrupting or destroying the data of other users | X | | | X | | | | X |
| Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature | | X | X | | X | | | X |
| Continued infringements of the above, following previous warnings or sanctions | | X | | X | | | | X |
| Actions which could bring the school into disrepute or breach the integrity of the ethos of the school | | X | | X | | | | X |
| Using proxy sites or other means to subvert the school's filtering system | | X | | | X | X | | X |
| Accidentally accessing offensive or pornographic material and failing to report the incident | | X | | X | X | | X | |
| Deliberately accessing or trying to access offensive or pornographic material | | X | | | X | | | X |
| Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act | | X | | | | | | X |

Staff actions and consequences

| Incidents: | Refer to line manager | Refer to Headteacher | Refer to Local Authority / HR | Refer to Police | Refer to Technical Support Staff for action re filtering etc. | Warning | Suspension | Disciplinary action |
|---|-----------------------|----------------------|-------------------------------|-----------------|---|---------|------------|---------------------|
| Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities). | X | X | X | X | | | | X |
| Inappropriate personal use of the internet / social media / personal email | X | X | | | | X | | |
| Unauthorised downloading or uploading of files | X | | | | X | X | | |
| Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account | X | | | | X | X | | |
| Careless use of personal data e.g. holding or transferring data in an insecure manner | X | | | | | X | | |
| Deliberate actions to breach data protection or network security rules | | X | X | | X | X | | X |
| Corrupting or destroying the data of other users or causing deliberate damage to hardware or software | | X | X | | X | X | | X |
| Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature | | X | X | X | | | X | X |
| Using personal email / social networking / instant messaging / text messaging to carry | | X | X | | | | | X |

| | | | | | | | | |
|---|---|---|---|---|--|---|---|---|
| out digital communications with students | | | | | | | | |
| Actions which could compromise the staff member's professional standing | | X | X | | | | | X |
| Actions which could bring the school into disrepute or breach the integrity of the ethos of the school | | X | X | | | | X | |
| Using proxy sites or other means to subvert the school's filtering system | X | | | | | X | | |
| Accidentally accessing offensive or pornographic material and failing to report the incident to the online safety coordinator / network manager | | X | | | | | | X |
| Deliberately accessing or trying to access offensive or pornographic material | | X | X | X | | | X | |
| Breaching copyright or licensing regulations | | X | X | | | | | X |
| Continued infringements of the above, following previous warnings or sanctions | | X | X | | | | X | X |