# Trinity and St.Michael's

## Online Safety Policy

"Don't withhold good from someone who deserves it, when it is in your power to do so."
Proverbs 3 Verse 27

Do everything in


1 Corinthians 16:13-14

Do everything in


1 Corinthians 16:13-14

# Introduction

*Therefore, if anyone is in Christ, the **new** creation has come: The old has gone, the **new** is here!*
*2 Corinthians 5:17*

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school and it is integral that we, as Christians, embrace what is new and do not shy away from it. However, in order for anything to be embraced, it first must be understood.

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. Children and young people should have an entitlement to safe Internet access at all times and, when using the internet, show **respect** and **compassion** in all they do.

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of a wider duty of care to which all who work in schools are bound. The school's Online Safety Policy should help to ensure safe and appropriate use. The development and implementation of such a strategy should involve all the stakeholders in a child's education from the head teacher and governors to the senior leaders and classroom teachers, support staff, parents, members of the community and the pupils themselves.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote student/pupil achievement. However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to/loss of/ sharing of personal information, whether willingly or through phishing
- The risk of being subject to grooming by those with whom they make contact on the internet
- The sharing/distribution of personal images without an individual's consent or knowledge
- Inappropriate communication/contact with others, including strangers
- Cyber bullying
- Access to unsuitable video/internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use, which may impact on the social and emotional development and learning of the young person

Many of these risks reflect situations in the off-line world and it is essential that this policy be used in conjunction with other school policies including Child Protection, Data Protection and Whole School Behaviour policies for example.

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision, to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

The school must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce those risks. The Online Safety policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents/carers) to be responsible users and stay safe while using the Internet and other communications technologies for educational, personal and recreational use.

## Associated School Policies

This policy should be read in conjunction with the following school policies/procedures:

- Policy on the use of Social Networking sites and other Social Media
- Safeguarding and Child Protection Policy
- GDPR Notice for Pupils and Families
- Health and Safety Policy
- Behaviour Management Policy
- Anti-Bullying Policy

The school will monitor the impact of the policy using:

- *Logs of reported incidents on our CPOMS system*
- *Pupil and staff interviews*
- *Stakeholder Feedback*

## Scope of Policy

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

The Education and Inspection Act 2006 empowers head teachers to such an 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 cyber bullying, or other Online Safety related incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

The school will deal with such incidents within this policy and the whole school Behaviour Management Policy which includes anti-bullying and will, where known, inform parents/carers of incidents of inappropriate Online Safety behaviour that take place out of school.

## Roles and Responsibilities

The following section outlines the roles and responsibilities for Online Safety of individuals and groups within the school:

### Governors

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. The Online Safety Governor will carry this out as part of their role. The role of the Online Safety Governor will include:

- Regular meetings with the Online Safety co-ordinator
- Reporting to relevant Governors meetings

## Headteacher

- The Headteacher has a duty of care for ensuring the safety (including Online Safety) of members of the school community, though the day-to-day responsibilities for Online Safety will be delegated to the Online Safety co-ordinator. However, all staff would be expected to have a shared responsibility.
- The Headteacher and Deputy Headteacher will be aware of the procedures to be followed in the event of a serious Online Safety allegation being made against a member of staff (see flowchart on dealing with Online Safety incidents on page 10, and relevant Local Authority HR/school disciplinary procedures).
- The Headteacher is responsible for ensuring that the Online Safety co-ordinator and relevant staff receive appropriate CPD to enable them to carry out their Online Safety roles and train other colleagues, as relevant
- The Headteacher and Governors will receive regular monitoring reports from the Online Safety co-ordinator

## Online Safety Co-ordinator

The designated school Online Safety co-ordinator is Mr G Hughes

He:

- takes day-to-day responsibility for Online Safety issues and has a leading role in establishing and reviewing the school Online 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
- ensures that the DSP is alerted to potential serious Child Protection issues
- facilitates training and advice for staff
- liaises with the Local Authority (when appropriate)
- liaises with the school IT provider & technician
- receives reports of Online Safety incidents through the CPOMS system
- attends relevant meetings/committees
- reports regularly to school staff
- keeps parents informed re potential issues

## Computing Subject Lead

The Computing Subject Leader (Mr G Hughes) with the support of the IT Technician, 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 outlined in the school Online Safety/Acceptable Use Policy and any Local Authority/Government Online Safety guidance
- that users may only access the networks and devices through a properly enforced password protection policy, in which staff are encouraged to change their passwords regularly
- that the school filtering system is fit for purpose
- 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 / website / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the relevant staff for investigation/ action/ sanction

## Teaching and Support 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 / Agreement (AUP)
- they immediately report any suspected misuse or problem to the Online Safety Co-ordinator for investigation/ action / sanction
- All digital communications with students / pupils / 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
- pupils understand and follow the Online Safety and Acceptable Use Policies
- they monitor computing activity in lessons and extra-curricular activities
- in lessons where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and to processes in place for dealing with any unsuitable material that is found in internet searches

## Designated Person for Child Protection

Is made aware of 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

## Pupils

Taking into account the age and level of understanding, our pupils:

- will be guided in using the school ICT systems in accordance with the Pupil Acceptable Use Policy/Agreement.
- need to understand the importance of reporting inappropriate content
- should know the importance of adopting good Online Safety practices at home

## 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. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through information guidance on Online Safety. Parents and carers will be responsible for:

- endorsing (by signature) the Pupil Acceptable Use Policy
- ensuring that they themselves do not use the internet/ social network sites/ other forms of technical communication in an inappropriate or defamatory way.

*"Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it."*

*(Byron Report, 2008).*

Our school offers regular opportunities for parents/carers and the wider community to be informed about Online Safety by school newsletter, homework diaries and the school website.

## Community Users

Community Users who access school ICT systems/website will be expected to sign a AUP before being provided with access to school equipment or internet access.

## Pupils with Additional Needs

At our school we strive to meet the needs of every child and take into account that some of our children may require extra support or a personalised plan to ensure they are given appropriate access to Online Safety information.

- A fundamental part of teaching Online Safety is to check pupil's understanding and knowledge of general personal safety issues. Some pupils may need additional teaching that includes reminders and explicit prompts to link their existing knowledge of how to keep safe to the rules that will apply specifically to, for instance, internet use.
- It is usually helpful to present the rules as being linked to consequences such that cause-effect is taught rather than a list of procedures. This is achieved carefully so as to use realistic and practical examples of what might happen if… without frightening pupils.

# Managing Information Systems

## Maintaining Information Systems Security

- The security of the school information systems and users will be reviewed regularly
- Virus protection will be updated regularly
- Portable media may not be used without specific permission followed by an antivirus/malware scan
- Unapproved software will not be allowed in work areas or attached to e-mail
- Files held on the school's network will be regularly checked
- The Computing Subject Leader will review system capacity regularly
- Use of user logins and passwords to access the school network will be enforced – see below
- Staff will use encryption software to ensure any data that contains pupil information is secure

## Password Security

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 access another user's files without permission
- Access to personal data is securely controlled in line with the school's General Data Protection Policy

A safe and secure username/password system is essential if the above is to be established and will apply to all school ICT systems (including e-mail).

The management of password security will be the responsibility of the Computing Subject Leader.

## Responsibilities

- All staff will have responsibility for the security of their username and password, must not allow others to access the systems using their log-in details and must immediately report any suspicion or evidence that there has been a breach of security
- Staff must ensure that passwords are not automatically held on accounts – they must always be inputted each time

## Training / Awareness

It is essential that users are made aware of the need to keep passwords secure, and the risks attached to unauthorised access/data loss.

It is essential that users are made aware of the need to keep passwords secure, and the risks attached to unauthorised access/data loss.

Members of staff will be made aware of the school's password security procedures:

- At induction
- Through the schools Online Safety policy
- Through the Acceptable Use Agreement

Students will be made aware of the school's password procedures where appropriate (e.g. use of email / use of chromebooks).

## Auditing / Monitoring / Reporting / Review

The Computing Subject Leader will ensure that full records are kept of:

- User IDs and requests for password changes
- User log-ins
- Security incidents related to this policy
- Inappropriate searches made online

In the event of a serious security incident, the police may request and will be allowed access to passwords for encryption. Local Authority Auditors also have right of access to passwords for audit investigation purposes. User IDs and other security related information must be given the highest security classification and stored in a secure manner (school safe).

## E-mailing Personal, Sensitive, Confidential or Classified Information

Assess whether this information can realistically be sent using other secure means before considering sending via e-mail. E-mailing confidential data is not recommended and should be avoided wherever possible.

If this is not practical then the following procedure should be followed:

- Use of personal e-mail accounts to discuss school matters is strictly prohibited. Data should only be sent through an official school Office 365 e-mail account
- All data should be encrypted or password protected
- Exercise caution when sending the e-mail;
- Verify the details of the recipient via telephone
- Do not forward or copy the e-mail to any more recipients than is absolutely necessary
- Do not identify such information in the subject line
- Request confirmation of safe receipt

## Zombie Accounts

Any accounts held by staff that no longer holds a contract of employment at the school will be removed as soon as possible after they cease to work at the school by the Computing Subject Leader/Technical support staff. These will include email and any other application accessed on behalf of the school (e.g. Nearpod, Times Table Rockstars). School Office staff are responsible for ensuring that staff are added/removed from the Lancashire School Portal system as appropriate.

## Pupil email accounts

All pupils within school have an email address. It is up to staff when they feel it is appropriate that this address is shared but it is common practice for this to be given when the child moves in to Key Stage Two. Children must use their own email address when accessing Chromebooks.
Pupils will use set passwords as defined by school staff and these may not be changed without prior approval of the class teacher/Computing Subject Leader.
Pupils may access these accounts within or outside of school as required but must comply with the points set out below under the 'Use of Digital and Video Images'.

## 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 cyber bullying 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 possible that employers may 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 / pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.
- 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 is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / 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. 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 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, blog or social media site, particularly in association with photographs
- Written permission from parents or carers will be obtained before photographs of students / pupils are published on the school website or any other social media platform
- Pupil's work can only be published with the permission of the pupil and parents/carers
- Teachers who record and distribute video lessons must ensure they are selective with who this is shared with.
- When teachers teach using video software (e.g. Zoom / Teams) they must take every effort to ensure that people outside of their class are not able to access the session through appropriate password and vetting of individuals attending through the login screen.

## Managing Social Networking, Social Media and Personal Publishing Sites

Many adults and pupils regularly use Social Network sites such as Facebook, Twitter, Snapchat or Instagram although the minimum age for registering for some of these excludes primary school pupils. These communication tools are, by default, 'blocked' through the Internet filtering system for direct use by pupils in Lancashire schools. However, comments made outside school on these sites may contravene confidentiality or bring the school or staff into disrepute.

**In our school we follow and adhere to the Local Authority Model Policy. However, school also requires that all adults working within school adhere to the additional statements below on what we consider to be acceptable and unacceptable use of Social Network sites:**

## Adults working/supporting in school are aware that:

- they must not give personal contact details to pupils or parents/carers including mobile telephone numbers, details of any blogs or personal websites
- adults must not communicate with pupils using any digital technology where the content of the communication may be considered inappropriate or misinterpreted
- if a Social Network site is used, details must not be shared with pupils and school recommends that privacy settings be set at maximum
- they are strongly advised not to add current or former pupils as 'friends' on any social network site
- school does not approve of members of staff adding parents as 'friends'
- no derogatory comments about our school should be made
- no comments about a member of staff within our school should be made

- no comments about a pupil within our school (including the use of pseudonyms/abbreviations) should be made
- no comment on any information about our school in general should be made outside of the official school social media channels
- no posting of photographs relating to children in our school or its pupils outside of official school social media channels
- no accessing of any Social Networking Site for personal use via school equipment is permitted
- no access of personal social media accounts during working hours

Inappropriate use of Social Networking Sites may lead to Disciplinary Procedures. Staff are reminded that whatever means of communication they use they should always conduct themselves in a professional manner. If content is made available on the web it is available for everyone to see and remains there forever.

## Parents/Carers need to be aware that:

- access to most social networking sites is limited to children aged 13 or over e.g. Instagram, Facebook
- parents are strongly advised to monitor their child's use to ensure they remain safe
- school does not approve of the underage use of these sites by pupils
- concerns regarding pupils' use of social networking, social media and publishing sites (in or out of school) will be raised with parents/carers
- inappropriate use of these sites (in or out of school) may result in action being taken by school as part of the wider behaviour management policy
- Advice for parents on keeping children safe online will be made available on the schools' website and via the school's Twitter for parents to consider
- the use of other school pupils' names in association with the school is not condoned and may result in breaches of confidentiality and safety for those pupils

## Managing Filtering

Currently the management of the schools' Internet filtering is undertaken as part of the Local Authority Netsweeper filtering service. Any issues relating to this system should be forwarded to the Computing Subject Leader/IT Technician for action. To ensure that this filtering system does not cause 'over blocking' and thus limit the ability of teachers to provide a broad curriculum or achieve specific learning objectives, teachers may on occasion, request that specific restrictions are removed by the Computing Subject Leader.

## Managing Live Video Lessons and Meetings

- Currently the school uses Zoom and, where asked to, Windows Teams to take part and host video lessons, worship and meetings (such as staff meetings and parents' evenings).
- The school has access to two Zoom accounts held by the head and Computing Subject Lead.
- Pass codes are required for these sessions and are sent via email.
- If a live session needs to be recorded (e.g. due to students being unable to participate live) those accessing live will be told this is the case and advised to turn their cameras off.
- If an individual is being disruptive during a live session it is at the teacher's discretion (following a warning) as to whether they are disconnected from the session.

## Managing Emerging Technologies

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

## Managing Social Media Accounts

All social media accounts associated with the school will be required to comply with all the requirements for image use outlined in this policy. Teachers and Teaching Assistants can post to the official school Social Media accounts with day-to-day guidance provided by the Computing Subject Leader.

## Data Protection

Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulations 2018.

Further details can be found in the School General Data Protection Policy.

**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.

## Disposal of Redundant ICT Equipment

- The Computing Lead will first check if any classes wish to keep redundant equipment as part of their computing sessions.
- All redundant ICT equipment will be disposed of through an authorised agency and comply with all electrical waste regulations.
- All equipment will be checked and wiped/hard drives removed by the school IT Technician.
- All disposals will be recorded within the school Hardware files.
- A written receipt for all disposals will be held on file for a minimum of five years.

# Policy Decisions

## Curriculum Support/Adult Training

- Children will, as part of a broad and balanced curriculum, be made aware of online risks and taught how to stay safe online
- Specific reference to online safety will be both explicitly and implicitly referenced through the school computing curriculum. Further opportunities to consider online safety will be explored through PSRHE lessons and Key Stage sessions
- School staff will receive annual training on the procedures to follow should they have any concerns regarding a pupil's online activity

## Authorised Internet Access

- All staff will read and sign the *appropriate* Acceptable Use Policy before using any school ICT resources
- Parents will be asked to read and sign the School Acceptable Use Policy for pupil access
- All visitors to the school site who require access to the school network or internet access will be asked to read and sign the appropriate Acceptable Use Policy
- Use of the Staff Wi-Fi network will only be approved for users who are working within school
- Parents will be informed that pupils' will be provided with supervised Internet access appropriate to their age and ability
- When considering access for vulnerable members of the school community (such as those with Special Educational Needs) the school will make decisions based on the specific needs and understanding of the pupil(s).

## Assessing Risks

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor the LA can accept liability for the material accessed, or any consequences resulting from Internet use.
- The school will audit ICT to establish if the Online Safety policy is adequate and that the implementation of the Online Safety policy is appropriate
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to Lancashire Police.

## 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:

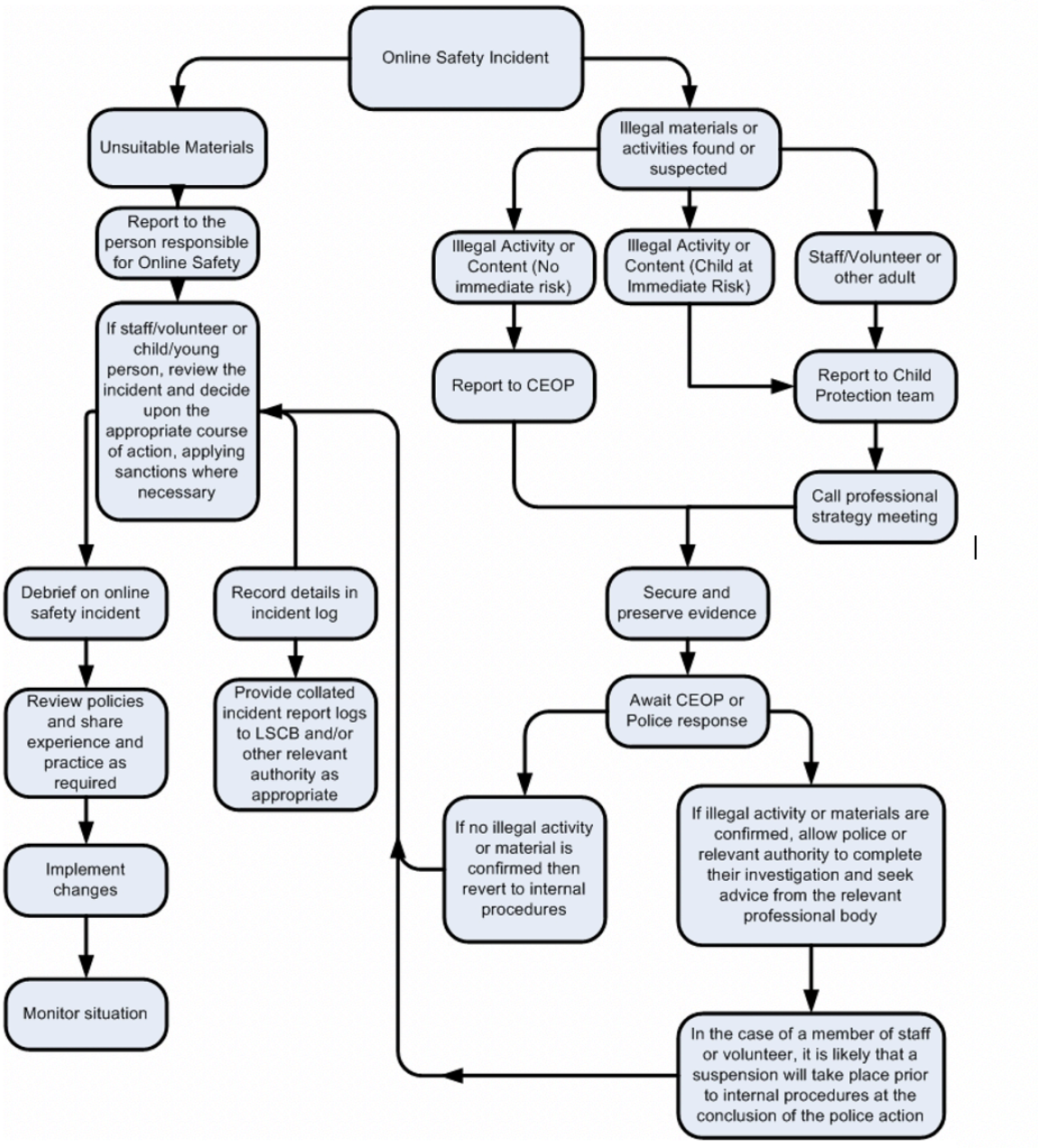
| User Actions | | Acceptable | Acceptable at certain times | Acceptable for nominated users | Unacceptable | Unacceptable and illegal |
|---|---|---|---|---|---|---|
| Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals 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 | |
| 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 | |
| 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 eg Youtube | | | | X | | |

# Reporting Incidents of Concern

If any apparent or actual misuse appears to have occurred, school will follow the procedure outlined below:

- Any incidents will be recorded through the schools CPOMS electronic system with a copy issued to the Online Safety Co-ordinator
- The Designated Person for Child Protection will be informed of any Online Safety incidents involving Child Protection concerns
- The school will manage Online Safety incidents in accordance with the school discipline/behaviour management policy
- The school will inform parents/carers of any incidents of concern as and when required

The school will follow the procedure outlined in the table below:



# Reporting Incidents of Concern cont.

It is more likely that 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. See below tables for examples of inappropriate use and sanction procedures.

| Student/Pupils Incident | Actions / Sanctions |
|---|---|
| Unauthorised use of non-educational sites during lessons | Any pupil action considered illegal would be referred to the Class Teacher, Headteacher & consequently the Police.<br><br>Inappropriate actions, as per the examples here, will be dealt with by the class teacher and/or KS Leader resulting in a warning and possible sanction (depending on nature of particular incident).<br><br>Depending on the seriousness of the action/level of intent, parents & Headteacher may also be informed.<br><br>If inappropriate action is repeated then incident reported to KS Leader, for further sanction and possible removal of network/internet access rights. Parents informed.<br><br>If inappropriate actions continue or are considered particularly serious then they will be referred to the Headteacher.<br><br>In all situations a record of the action and sanction should be added to CPOMS and the school Online Safety Co-ordinator informed. |
| 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 student's / 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 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 | |

| STAFF Incidents | Actions / Sanctions |
|---|---|
| **Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section).** | **In this instance a direct referral to the Headteacher would be made.** |
| Inappropriate personal use of the internet / social media / personal email | Any example of inappropriate use, as listed here to the left, would result in the matter being referred to their Line Manager in the first instance with an appropriate warning sanction.<br><br>If infringement continues then the matter would be referred to the Deputy Headteacher and/or Headteacher (and DSP if a Child Protection issue) with the strong possibility of suspension and/or disciplinary action.<br><br>In all cases, details will be recorded and the school Online Safety Co-ordinator notified by the Headteacher if relevant. |
| Unauthorised downloading or uploading of files | |
| 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 | |
| Careless use of personal data e.g. holding or transferring data in an insecure manner | |
| Deliberate actions to breach data protection or network security rules | |
| Corrupting or destroying the data of other users or causing deliberate damage to hardware or software | |
| Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature | |
| Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with pupils | |
| Actions which could compromise the staff member's professional standing | |
| 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 | |
| Breaching copyright or licensing regulations | |
| Continued infringements of the above, following previous warnings or sanctions | |

# Managing Cyber Bullying

- Cyber bullying (along with all forms of bullying) of any member of the school community will not be tolerated
- All incidents of bullying will be dealt with as defined in the School's Anti-Bullying Policy (please see the Anti-Bullying Policy for more details)
- Some types of harassing or threatening behaviour, or communications are a criminal offence (under, for example, the Protection from Harassment Act 1997; the Malicious Communications Act 1988 and the Communications Act 1988) For example, it is an offence for a person to send an electronic communication to another person with the intent to cause distress or anxiety, or a communication which is indecent or grossly offensive, a threat, or to send information which is false and believed to be false by the sender. If school have reason to believe any of the above to be the case, the headteacher may deem it necessary to refer the matter to the Police.

It is very difficult for school to 'police' Internet use outside of school, and as such parents are expected to be responsible for monitoring their child's exposure to, and use of, the Internet. If parents have reason to believe any of the above offences to have occurred, then they are advised to refer the matter to the Police. If the perpetrators are pupils at the school then parents should also inform school.

# Managing Mobile Phones and Personal Devices

## Pupils

- The sending of inappropriate messages via mobile phones or personal devices is forbidden by any member of the school community and any breaches will be dealt with as part of the school disciplinary/behaviour policies
- Pupils are not allowed to use phones at school and are discouraged from bringing them onto the school premises
- Electronic devices are allowed for older pupils if they walk home from school.
- Electronic devices brought into school are the responsibility of the user. The school accepts no responsibility for the loss, theft or damage of such items. Nor will the school accept responsibility for the adverse health effects caused by any such devices either potential or actual.

## Staff

- Mobile phones and personal devices will not be used during lessons or formal school time. They should be switched off or left on silent during these periods and not be visible within the classroom **(urgent or important communication can be received via the School Office)**
- Adults working in school are expected to place their mobile phones in a safe place away from children.
- Staff are not permitted to use their personal devices for contacting children, young people and their families within or outside of the setting in a professional capacity. (However, staff on school trips or activities away from the school base are permitted to use personal devices to contact parents if no school device is available)
- Staff must use a school phone where contact with pupils/carers is required
- Staff are not allowed to use personal devices to take photos or videos of pupils

## Managing Filtering

- School acknowledges that there may be **rare** occasions when an adult in school requires to use their personal phone. **In this event it is expected that the device is used in private and not in the staffroom or when children are present.** Line managers are expected to remind other adults if it becomes apparent that this rule is being breached.
- School provides computer equipment for teaching staff, supply teachers, student teachers and HLTA staff to use on a day-to-day basis when leading lessons. The use of personal computer equipment is not permitted within school.

## Discussing Policy with Staff

- This policy will be formally discussed with all staff on at least an annual basis
- This policy will be part of a package of policies that all new members of staff must read when they join school
- To protect all staff and pupils, the school will implement Acceptable Use Policies
- Up to date and appropriate training for staff in responsible Internet use will be provided for all members of staff
- Staff will be made aware that all Internet traffic is monitored and can be traced back to an individual user
- All staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or school into disrepute, or if something is felt to have undermined confidence in their professional abilities.
- Discretion and professional conduct is essential at all times