**ONLINE SAFETY POLICY**

| | |
|---|---|
| Last Review: | Feb 2026 |
| Committee: | PSW |
| Date Ratified: | 03/02/2026 |

## 1. Introduction

**This policy should be read in conjunction with Keeping Children Safe in Education (latest version) and reflects the school's statutory safeguarding responsibilities, including those relating to online safety.**

1.1. The growth of the internet and the development of mobile technology has created an exciting and stimulating world with great opportunities for students to explore, interact, learn and enjoy social interaction online. It is now an integral to all our lives. Students will need to develop high-level ICT skills, not only to maximise their potential use as a learning tool, but also to prepare themselves as lifelong learners and for future employment.

1.2. However, the importance of treating online safety as an ever-present serious safeguarding issue is recognised. It is important to protect and educate both students and staff and have supportive mechanisms, policies and protocols in place to protect and support the school community both in and outside of school.

1.3. The safeguarding aspects of online safety are evident in all our ICT/safeguarding policies and procedures throughout the school and it is essential that this constantly developing area of technology is kept under review. As with all other risks it is impossible to eliminate those risks completely. It is therefore essential to support all stakeholders in acquiring the skills to remain safe whilst accessing this technology.

1.4. This policy should be read in conjunction with the following policies -

- Information and Communication Technologies and Acceptable Use
- Safeguarding and Child Protection
- Anti-bullying
- Behaviour for Learning
- Code of Conduct for staff
- Whistleblowing
- Mobile Phone and Electronic Devises
- Privacy
- Data Protection
- BYOD
- Other procedures to reflect how the school deals with online safety issues on a daily basis.

## 2. Objectives and Targets

2.1 This policy is aimed at making the use of electronic communication at Oldfield School as safe as possible. It applies to all members of the school community (including staff, students, volunteers, parents/carers, visitors, community users) who have access to, and are users of, school ICT systems, both in and out of school.

2.2 This policy aims to support the school community in understanding their responsibilities in ensuring safety when using technologies whilst fully exploiting the power of these technologies to enhance educational outcomes.

2.3 Additionally it aims to build both an infrastructure and culture of online safety.

## 3. Action Plan

3.1 The school will deal with any online safety incidents which arise by invoking this policy, other ICT policies and the associated Behaviour for Learning and Anti-Bullying policies. The school will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place in and outside of school and take appropriate action.

3.2 The following sections outline:

- The roles and responsibilities for online safety of individuals and groups within the school, and how they will receive education/training to fulfil those roles (Appendix 1)
- How the infrastructure is managed (Appendix 2)
- How online safety is considered in the curriculum.
- The protocols on using digital images.
- The protocols for handling electronic communication.
- Training and communication for all stakeholders
- Awareness of and dealing with inappropriate use of electronic media (Appendix 3 & 4)
- Advice and support for all stakeholders (Appendix 5 & 6)

### 4. Curriculum

4.1 While 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. Online safety education will be provided in the following ways:

- A planned online safety programme is provided as part of ICT/PSHE/other lessons – this includes both the use of ICT and new technologies in and outside of school.
- Key online safety messages are reinforced as part of a planned programme of assemblies and tutorial/pastoral activities.
- Students are taught in all lessons to be critically aware of the materials/content they access online and are guided to validate the accuracy of information.
- Students are taught about emerging online risks, including livestreaming, image-based abuse, harmful online challenges, and the responsible use of AI-generated content, and how to seek help if they are concerned.
- Students are taught the importance of not sharing personal information and photographs over the internet.
- Students are helped to understand the need for the Student Acceptable Computer Usage Agreement annually and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school. All students receive the Acceptable Use Agreement at the beginning of the school year and acknowledge their consent when they log on to the school system. This policy is also shared with Parents/Carers when they join the school.
- Students are taught to acknowledge the source of any information used and to respect copyright when using material accessed on the internet.
- Rules for use of ICT systems/internet are posted in all relevant rooms and/or displayed on log-on screens.

4.2 Online safety is a focus in all areas of the curriculum and staff reinforce online safety messages in the use of ICT across the curriculum. For example:

- In lessons where internet use is pre-planned, students are guided to sites checked as suitable for their use and processes are in place for dealing with any unsuitable material that is found in internet searches.
- Staff emphasise the positive use of technology, rather than the negative, to promote self-esteem, assertiveness and encourage an inquisitive learning environment.
- Where students are allowed to search the internet freely, e.g. using search engines, staff are vigilant in monitoring the content of the websites the students visit.
- Staff encourage students to use specific terms to reduce the likelihood of coming across unsuitable material. Processes are in place for dealing with any unsuitable material that is found in internet searches.
- 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 can request that the ICT Technicians temporarily remove those sites from the filtered list for the period of study. Any request to do so will be recorded, with clear reasons for the need.
- Students are taught in all lessons to be critically aware of the content they access on-line and are guided to validate the accuracy of information.
- Students are taught the importance of not sharing personal information and photographs over the internet.

## 5. Data Protection

5.1 Personal data will be recorded, processed, transferred and made available in accordance with the Data Protection Act 2018 and the UK General Data Protection Regulation (UK GDPR). **Refer to the ICT policy and Data Protection and Information Security policy.**

## 6. Publishing Digital and Video Images

6.1 When using digital images, staff inform and educate students about the risks associated with taking, using, sharing, publishing and distributing images. In particular, they recognise the risks attached to publishing their own images on the internet, e.g. on social networking sites.

6.2 Staff 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. All photographs and video taken within school are used to support learning experiences across the curriculum, as well as to provide information about the school on the website.

6.3 Any images should only be taken on school equipment. Personal equipment of staff should *not* be used for such purposes.

6.4 Photographs published on the website, or elsewhere, that include students will be selected carefully and will comply with good practice guidance on the use of such images. Permission from parents or carers will be obtained and stored on SIMS when the student joins the school.

6.5 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 in the digital / video images.

6.6 We ask parents/carers to consider the purpose and impact of sharing photos or videos online. These are shown in **Appendix 7.**

6.7 Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.

## 7. Published content and the School Website

7.1 The contact details on the website will be the school address, email and telephone number.

7.2 Staff and students' personal information will not be published on the website.

## 8. Social networking

8.1 Students, parents and staff are advised on the safe use of social network spaces.

8.2 Staff are advised to use strong privacy settings if using social media. The personal use of email, social networking, social media and personal publishing sites will be discussed with staff as part of staff induction and relevant matters will be raised in staff meetings / ongoing staff training. Safe and professional behaviour is expected of all staff **(refer to Staff Code of Conduct policy).**

8.3 Students are taught to not give out personal and location details on social media and social networking sites. They will be encouraged to use nick-names and avatars.

## 9. Mobile Phones

9.1 Staff and volunteers are expected to model 'acceptable use' to students and to only use mobile phones during break, lunchtimes or during non-contact time and not use them while they are with children / discharging their professional duties.

9.2 Staff should not use their personal mobile phone to contact students, parents/ carers except in exceptional circumstance when the number should be preceded by 141 to protect privacy.

9.3 Students are asked to ensure that all mobile phones are kept in bags and turned off during the school day **(refer to Mobile Phone policy).**

## 10. Communications

10.1 When using communication technologies, the school considers the following as good practice;

- All students read, accept and adhere to the Acceptable Use Policy at the start of the academic year or when they join the School and thereafter every 4 weeks.
- The official school email service is regarded as safe and secure and is monitored.
- Users are expected to know and understand school policies on email, social media and other relevant electronic devices protocols.
- Users must immediately report to a Designated Safeguarding Lead (DSL) in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature. Users must not respond to any such email but must follow the procedures as set out in this policy.
- Any digital communication between staff and students or parents/carers must be professional in tone and content. A copy of any such communication should be kept. Personal addresses, mobiles etc. must not be used for these communications.
- Personal information should not be posted on the school website and only official school email addresses should be used to identify members of staff. A breach of any of this guidance may result in disciplinary action.
- Staff are advised to use strong privacy settings when using social media.
- The School controls the use of social media and social networking sites unless educational and promotes appropriate use outside of school following social media sites guidelines of use/age categories.
- Students are taught to not give out personal and location details on social media and social networking sites. They will be encouraged to use nicknames and avatars.

## 11. Assessing Risks and Reporting Incidents

11.1 The School recognises that the breadth of issues within online safety is considerable, but can be categorised into 3 areas of risk:

- content: being exposed to illegal, inappropriate or harmful material; for example pornography, fake news, racist or radical and extremist views; livestreamed content and live video platforms; AI-generated or manipulated content, including deepfakes.
- contact: being subjected to harmful online interaction with other users; for example commercial advertising as well as adults posing as children or young adults; pressure or coercion during livestreams or private video interactions; grooming through gaming platforms or social media.
- conduct: personal online behaviour that increases the likelihood of, or causes, harm; for example making, sending and receiving explicit images, or online bullying; image-based abuse, including the non-consensual sharing of images or videos; participation in harmful online challenges.

11.2 Staff ensure that technology is being used appropriately to support learning. However, due to the global and connected nature of the internet content, it is not possible to guarantee access to unsuitable material will never occur via a school computer. The School cannot accept liability for the material accessed, or any consequences resulting from internet use.

11.3 Any student user found to be in violation of these guidelines will be subject to school discipline procedures. Repeated violations would cause that user to be banned from using the internet in school. In the case of adults, they could be banned from working with children.

11.4 Certain activities are referred to in the acceptable computer usage agreements as being inappropriate in a school context and users must not engage in these activities in school or outside school when using school equipment or systems.

11.5. The school policies on safeguarding and child protection, staff code of conduct and online safety *must be* followed if any apparent, suspected or actual misuse appears to involve illegal or inappropriate activity e.g.:

- Child sexual abuse images.
- Adult material which potentially breaches the Obscene Publications Act.
- Criminally racist material.
- Other criminal conduct, activity or materials.
- Any actions online that impact on the school and can potentially lower the school's (or someone in the school's) reputation in some way or are deemed as being inappropriate will always be responded to.

11.6 In the event that any member of staff, student or parent/carer is found to be posting libellous or inflammatory comments on Facebook or other social networking sites, this will be addressed by the school in the first instance. If appropriate, disciplinary action will result. However, where necessary, the police will be involved and/or legal action pursued. The school will use Criminal Prosecution Service guidance '*Guidelines on prosecuting cases involving communications sent via social media'* when making decisions in relation to cases where it is alleged that criminal offences have been committed by the sending of a communication via social media.

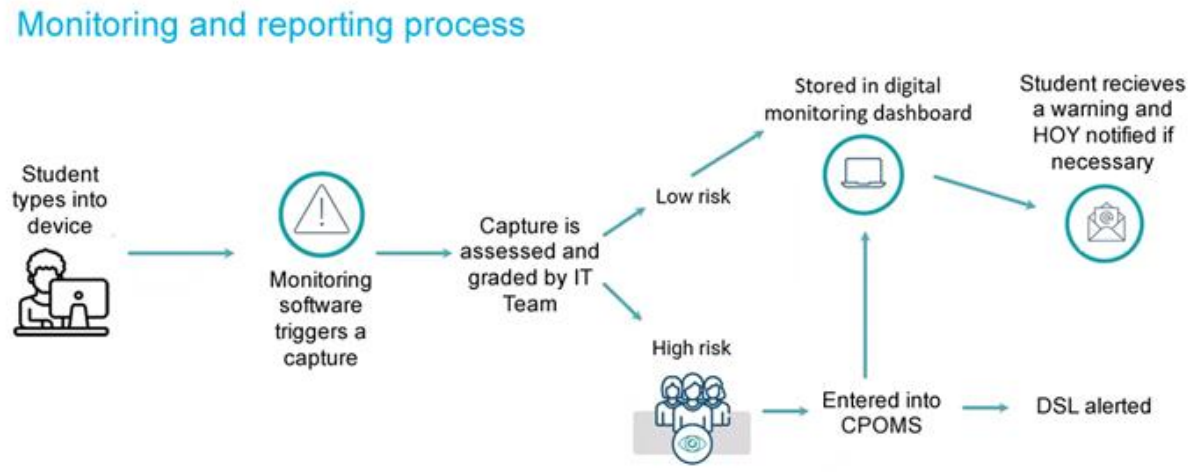
11.7. Should any serious online safety incidents take place, the appropriate external authorities will be informed (e.g. local area designated safeguarding officer, police etc.).

## 12. Managing Filtering and Monitoring

12.1 Content accessed through the School's internet system is managed and filtered by SWGfl (South West Grid for Learning).

Any inappropriate content must be reported to the Assistant Headteacher : Inclusion. Procedures will be followed to report inappropriate content to appropriate outside agencies. The number of incidents is reported to the Personnel and Welfare Committee three times a year.

12.2 Classroom.cloud is the school's primary monitoring platform.




## 13. Communicating with Parents

13.1 Parents will be invited to attend a meeting on Online Safety held either in School, virtually or with other local schools where appropriate. These will reinforce the key Online Safety messages from this policy and provide parents with information to support all children (and the wider school community) in staying safe as they use the internet and associated technologies.

13.2 On a student's entry to the school, the Student Acceptable Use policy will be shared with parents/carers and then again at the start of each key stage. Parents are given the opportunity to raise any queries regarding the policy at these times.

13.3 As part of the Online Safety curriculum, children will also receive any relevant information available to share with their family.

13.4 Where specific advice is received from time to time through external sources it will be passed on to parents through school induction, events, newsletters, emails and school website.

## 14. Training

14.1 All staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be delivered as follows:

- A planned programme of formal online safety training will be made available to staff via safeguarding updates/briefings.

- The Assistant Headteacher : Teaching and Learning monitors online safety training needs of all staff annually. CPD opportunities are provided to meet these needs either through in-house training or bespoke external courses.

- 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 usage policies.

14.2 The Assistant Headteacher: Inclusion will receive training at regular intervals (at least annually) and by reviewing national / local guidance documents.

14.3 The DSL and/or IT technicians provide additional support/advice/guidance/ training to individuals and whole staff body when required with regards to Online Safety.

14.4 Governors should take part in online safety training/awareness sessions, with particular importance to members of the governing body responsible for safeguarding / ICT / Health and Safety.

14.5 Parents /carers should be provided with information about the school's Online and Acceptable Use policies and how to help keep young people safe when using ICT at home. An information evening will be held annually to provide support/advice for parents.

## 15. Monitoring and reviewing

15.1 This policy will be reviewed annually by the Governing Body.

15.2 The school will monitor the impact of the policy using:

- Logs of reported incidents via CPOMS.
- Monitoring logs of internet activity.
- Surveys/questionnaires of students
- Feedback from parents/carers and staff

15.3 The policy will be reviewed in the light of any incidents that have taken place, significant new developments in the use of the technologies, or perceived new threats to online safety.

## Appendix 1 - Roles and Responsibilities

**Roles and Responsibilities - Governing Body**

- Will discuss, review and endorse agreed strategies via the Personnel and Student Welfare Committee and the Safeguarding Report on the workings of this policy.

**Roles and Responsibilities – Headteacher and SLT**

- The headteacher is responsible for ensuring the online safety of members of the school community.
- The Deputy Headteacher (Curriculum) and Assistant Headteacher (Inclusion) are aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff, including the headteacher.
- The Education and Inspections Act 2006 empowers the headteacher, to such extent as is reasonable, to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other online safety incidents covered by this policy, even though they may take place out of school, but are linked to membership of the school.

**Roles and Responsibilities – Designated Safeguarding Lead (DSL)**

The DSL is trained in online safety issues and will be aware of the potential for serious child protection issues to arise from:

- Sharing of personal data.
- Access to illegal/inappropriate materials.
- Inappropriate on-line contact with adults/strangers.
- Potential or actual incidents of grooming.
- Cyber-bullying.
- Sexting
- Potential exposure to radicalisation

The DSL -

- Takes day-to-day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policy and other related policies.
- Ensures that all members of 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 the local authority (LA).
- Liaises with school ICT technical staff.
- Liaises with the School Council and Staff Health and Safety committee. These bodies include online safety on their agendas and feedback their findings to the DSL.
- Reports regularly to SLT and the Governing Body.

**Roles and Responsibilities – ICT Technicians**

The ICT Technicians ensure:

- The school's ICT infrastructure is secure and is not open to misuse or malicious attack.
- The school meets the online safety technical requirements outlined in the relevant national/local guidance.
- Users may only access the school's networks through a properly enforced password protection policy.
- 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.
- The use of the network, internet, remote access and email is regularly monitored in order that any misuse or attempted misuse can be reported for investigation
- That monitoring software / systems are regularly updated.

**Roles and Responsibilities – Teaching and Support Staff**

Teaching and support colleagues are responsible for ensuring that:

- They have an up-to-date awareness of online safety matters and of the current school online safety policy.
- They have read and understood the relevant staff acceptable computer usage agreement and staff laptop usage agreement, as well as other related policies.
- They report any suspected misuse or problem to the relevant member of staff for investigation/action/sanction.
- Digital communications with students should be on a professional level and only carried out using official school systems.
- Students understand and follow the school online safety policy and the student acceptable computer usage policy.
- Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- They monitor ICT activity in lessons, extracurricular and extended school activities.
- They are aware of online safety issues related to the use of mobile phones, cameras and hand-held devices and that they monitor their use and implement current school policies with regard to these devices.
- They are aware of the online safety issues pertaining to email and social media usage.
- In lessons where internet use is pre-planned, students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

**Roles and Responsibilities – Students**

Students:

- Are responsible for using the school ICT systems in accordance with the student acceptable computer usage policy and agreement.
- 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 school policies on the use of mobile phones, digital cameras and hand-held devices.
- Will be expected to know and understand school policies on the taking/use of images and on cyber-bullying.
- Will develop a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Will 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.

**Roles and Responsibilities – 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. Parents and carers are responsible for endorsing the student acceptable computer usage agreement.

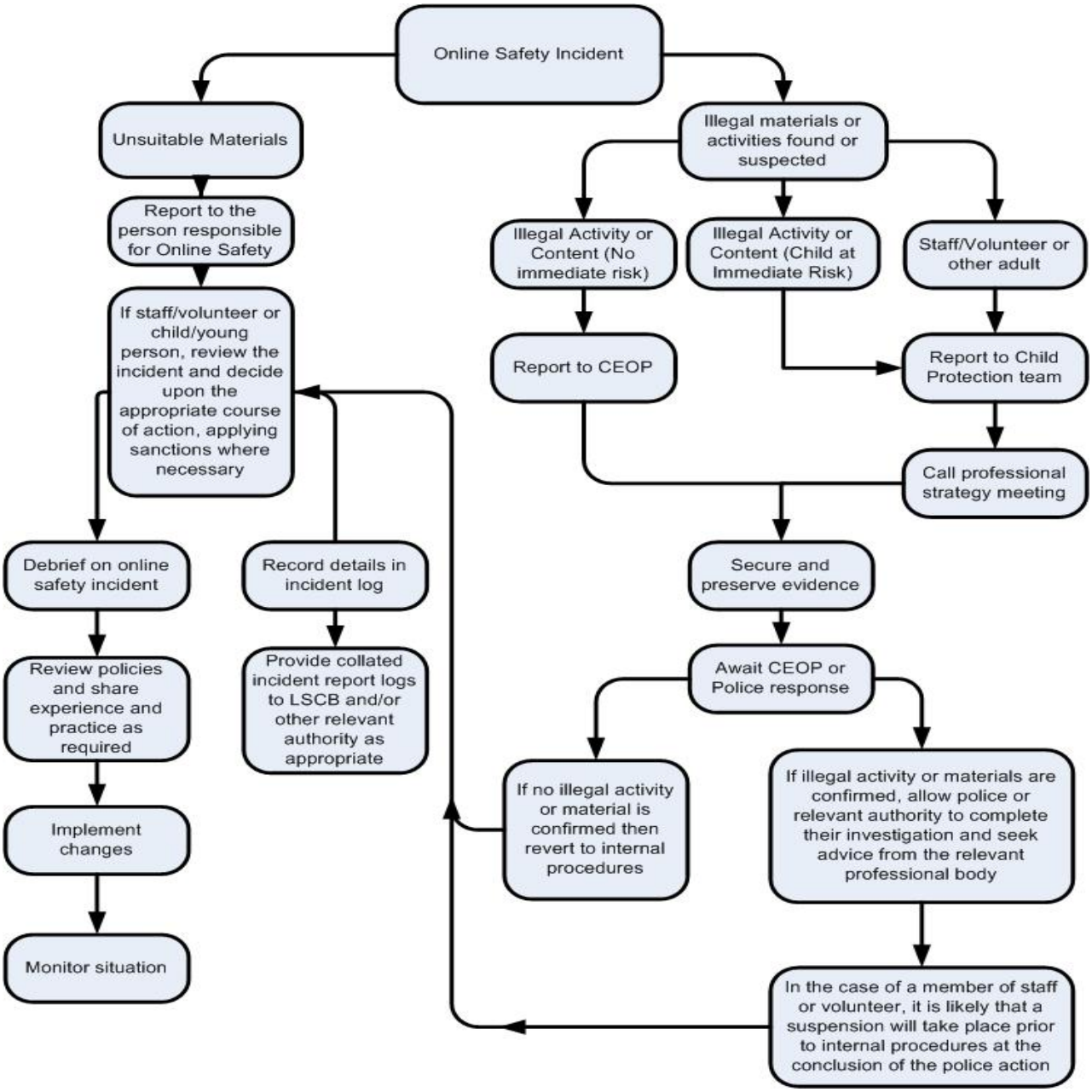
- Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through:

- Parents' evenings.
- Newsletters/Magazines.
- Letters.
- Website.
- Information about all relevant national/local e-safety campaigns/literature.
- Information about useful organisations /support services for reporting online safety issues **(see Appendix 2).**

## APPENDIX 2 Management of Infrastructure

- The school is 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.
- The school will also ensure that the relevant people named in Appendix 1 will be effective in carrying out their online safety responsibilities.
- School ICT systems are managed in ways that ensure that the school meets the online safety technical requirements outlined in the Online and ICT policies and any relevant LA online safety policy and guidance **(Refer to ICT policy)**
- All users have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users are recorded by the ICT Technicians and are reviewed regularly. All users are provided with a username and password by the ICT Technicians. Users are then responsible for the security of their username and password and must not allow other users to access the systems using their log on details. All must immediately report any suspicion or evidence that there has been a breach of security.
- The school maintains and supports the managed filtering service provided by the South West Grid for Learning. Any filtering issues are reported immediately to the ICT Technicians.
- School ICT Technicians regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the acceptable computer usage policy.
- The school infrastructure and individual workstations are protected by up-to-date anti-virus software.
- Personal data must not be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

**Appendix 3 - Responding to an online safety incident**



**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 involved in this process. 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.

## Appendix 4 - Using the Internet Safely

Annually students are reminded of the Acceptable Use Policy. This document is explained through the tutorial programme, subject teachers, and assemblies. Every time a student logs on in school or remotely a copy of this is displayed and agreed.

Students are taught to recognise the potential risks online including -

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of/ sharing of personal information including identity fraud.
- The risk of being subject to grooming by those with whom they make contact on the internet including the risks of CSE / Radicalisation.
- The sharing and distribution of personal images without an individual's consent or knowledge e.g. sexting/sending nudes.
- Cyberbullying.
- Access to unsuitable video, internet games or the illegal downloading of music/video files.
- The impact on a student's mental/physical wellbeing.
- Inappropriate communication / contact with others including strangers.
- Livestreaming and live video platforms.
- Image-based abuse, including sharing images without consent.
- Manipulated or AI-generated images and videos.
- Online dares or challenges that may cause physical or emotional harm.

**Managing incidents:**

- Students should report any concern or worry they have, regarding online safety to either their tutor, Head of Year, subject teacher or member of the Pastoral team or via the SWGFL Whisper / CEOP button on the school website.
- Staff should inform their line manager of any worries/concerns. If appropriate, the school's disciplinary procedures will be followed.
- The Designated Safeguarding Lead (DSL) should be informed if anyone's safety or wellbeing is considered to be at risk. All concerns are recorded on the school's CPOMS system. It may be necessary for the DSL to inform outside agencies e.g. the police/social care/ Local Designated Safeguarding Officer (LADO).

**Cyberbullying**

As students spend an increasing amount of time online the potential risk has increased. As a school we have a responsibility to regulate the behaviour of students both in and outside of school and will impose disciplinary sanctions for inappropriate behaviour. This includes incidents of cyber-bullying or other online safety incidents covered by this policy, which may take place outside of school but is 'brought into' school. However, parents are always advised to contact the police and the service provide if incident of cyber-bullying take place.

Cyberbullying is when one person or a group of people aim to threaten, tease or embarrass someone else by using a mobile phone, the internet or other technologies. Cyber bullying can take place through -

- Sending abusive instant messenger and chatroom messages about a person directly to them or to other people.
- Sending email that can be threatening or upsetting
- Using social networking sites (e.g. Snapchat) to set up false profiles to humiliate and abuse.
- Sending humiliating or abusive text or video messages, as well as photo messages and phone calls.
- Sharing photos and / or videos of a person without their informed consent and using those images to humiliate or abuse that person.

In the unfortunate case of a cyberbullying incident the school will follow the procedures as outlined in the Anti-Bullying and Safeguarding and Child Protection policies to support the individual(s) concerned and identify the main causes of the problems. All incidents of cyberbullying reported to the school will be documented, recorded and investigated. **(Refer to the Anti-Bullying and Safeguarding and Child Protection policies)**

Students, staff and parents/carers will be advised to keep a record of the bullying as evidence.

**Dealing with Cyber Bullying - Advice for parents**

- Report abuse to the providers of the service concerned.
- Print out and/or keep any abusive messages or images.
- Involve the police if it is persistent and inform school. The school's anti-bullying policy will then be followed.
- Parents can use the report an incident links on the school website to report an incident to CEOP.
- If bullying takes place outside of school, then it is the parents' responsibility to act in the first instance and if necessary inform the appropriate agencies.
- School will offer support and advice and take any reasonable action to ensure such incidents are not repeated and that it does not affect the education of all involved.

**Dealing with Cyber Bullying - Advice for Staff**

Staff should adhere to the guidance below and refer to anti-bullying and Safeguarding and Child Protection policies when dealing with an online safety incident.

- Reassure the individual(s) that they have done the right thing in reporting the incident.
- Acknowledge that it is difficult to tell but do not promise confidentiality.
- Reiterate that no one has the right to do that to others.
- Advise the victim not to retaliate or return the message but keep evidence (e.g. time and date, content of the message preferably on the device itself) and take this to a DSL/ Deputy DSL.
- Write down everything that has been disclosed as directed by the DSL/deputy DSL.

Note : This advice applies to both students and adults in the school community.

## Appendix 5 - Useful organisations/support services for reporting online safety issues

**Getting Help/Advice: for young people**

- ChildLine: Is a free 24/7 helpline for children and young people. Visit www.childline.org.uk or call 0800 1111. ChildLine is run by the NSPCC.
- Kooth: Kooth is an online counselling service for students to ask for advice about any online safety issue, https://www.kooth.com/
- Childnet; including Cyberbullying and Filtering guidance http://www.childnet.com/.
- Kidsmart - http://www.kidsmart.org.uk/
- ThinkuKnow – Very useful site for students for any online issue www.thinkuknow.co.uk

**Getting Help/Advice: for parents**

- Internet Matters (for parents) www.internetmatters.org
- NSPCC – Net Aware - http://www.net-aware.org.uk
- *Family Lives*: A charity providing help and support in all aspects of family life. They have a 24/7 free Parentline on 0808 8002222, or visit www.familylives.org.uk
- *Kidscape*: Is a leading anti-bullying charity, which provides a helpline for parents of children who have been bullied. From 10am to 8pm, on 08451 205204 www.kidscape.org.uk.
- *Commonsensemedia* provide independent reviews, age ratings, & other information about all types of media for children and their parents - Common Sense Media: Age-Based Media Reviews for Families
- *UK Internet Centre* – useful advice and tips for parents - UK Safer Internet Centre - Online Safety Tips, Advice and Resources | Safer Internet Centre

**Getting Help/Advice: for professionals working with children**

- *Professionals online safety helpline*: Helpline operated by the UK Safer Internet Centre offering professionals who work with children across the UK support, advice and mediation with on-line safety issues. The helpline can be contacted by email: helpline@saferinternet.org.uk or telephone on 0844 3814772 (calls on this number are charged at local call rate).

- UK Safer Internet Centre - https://www.saferinternet.org.uk/professionals-online-safety-helpline

- NSPCC - https://learning.nspcc.org.uk/research-resources/schools/e-safety-for-schools/

**Grooming or Other Illegal Behaviour**

If you want to report someone who is behaving suspiciously online towards a child, you should in an emergency contact the emergency services by calling 999, or otherwise make a report to *Child Exploitation Online Protection Centre (CEOP)*. See www.ceop.gov.uk.

**Criminal Content Online**

If you stumble across criminal content online, you should report this to the *Internet Watch Foundation (IWF)* at www.iwf.org.uk/report. Criminal content in the UK includes child sexual abuse images, criminally obscene adult content as well as non-photographic child sexual abuse images.

Online content which incites hatred on the grounds of race, religion and sexual orientation should be reported to *True Vision*, which tackles all forms of hate crime, including those on the grounds of disability and transgender identity. True Vision, at www.report-it.org.uk, will give you information on content which incites hatred and how to report it.

**Scams**

If you have been 'scammed, ripped off or conned' you can report to *Action Fraud* on 0300 123 2040 or http://www.actionfraud.police.uk. This service is run by the National Fraud Authority, the UK's government agency that helps coordinate the fight against fraud.

## Appendix 6 Sharing Digital Images and Video Online – A Parents' Guide

Before posting a photograph or video online please consider the following information:

- Some children and adults are at risk and MUST NOT have their image put online. Not all members of the school community will know who they are so always ask permission before sharing photos or videos online;

- Once posted and shared online any image or video can be copied and will stay online forever;

- Some people do not want their images online for personal or religious reasons;

- Some children, families and staff may have a complex family background which means that sharing their image online can have unforeseen consequences;

- In order to keep all members of the school community safe we must all 'think before we post' photos and videos online.

- Parental sharing can affect children as they grow up. Sharing photos and information online is permanent, and what can seem appropriate to share now may not be in the future.

- When posting a photograph or video a parent might be sharing more than what's in the post. As default, many cameras, phones and apps tag posts and photos with 'meta-data' which can include location details and other identifying information. This is potentially risky for any child, but poses particular risks for vulnerable children who could be sought online.

- Once information about a child is on the internet it can be difficult for them to control it and so we need to be considerate when we share things on their behalf. Respecting this right to a private life now, and in the future, is only good manners.

## Appendix 7 Government Legislation

The school complies with all current UK legislation and statutory guidance relating to online safety and safeguarding. This includes, but is not limited to:

- **Statutory safeguarding guidance**
- Keeping Children Safe in Education (latest version)
- Working Together to Safeguard Children
- **Data protection**
- Data Protection Act 2018
- UK General Data Protection Regulation (UK GDPR)
- **Education legislation**
- Education and Inspections Act 2006
- Education Act 2011 (searching and confiscation)
- **Online and communications legislation**
- Online Safety Act 2023
- Communications Act 2003
- Malicious Communications Act 1988
- Computer Misuse Act 1990
- **Criminal and safeguarding legislation**
- Sexual Offences Act 2003
- Criminal Justice and Courts Act 2015
- Voyeurism (Offences) Act 2019
- Protection from Harassment Act 1997
- **Filtering and monitoring**
- DfE Filtering and Monitoring Standards for Schools and Colleges