IMBERHORNE SCHOOL

Headteacher: Matthew Whatford

Online Safety Policy	
Date of review:	July 2025
Prepared by:	Emma Best
Approved by Governing Board:	17/07/2025
Policy based on:	Keeping Children Safe in Education
Date for next review:	July 2026
Links to other policies	Misuse of texts and images Anti-Bullying Policy Behaviour for Learning Policy Safeguarding and Child Protection Policy

Aims

Our schools aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Identify and support groups of pupils that are potentially at greater risk of harm online than others
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- Content - being exposed to illegal, inappropriate, or harmful content, for example: pornography, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, extremism, misinformation, disinformation (including fake news) and conspiracy theories.
- Contact – being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
- Conduct – online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying, and

- Commerce – risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).

Imberhorne Lane East Grinstead West Sussex RH19 1QY

T: 01342 323562 F: 01342 317366 E: info@imberhorne.co.uk www.imberhorne.co.uk

Legislation and guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities 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. This will be carried out by the Governors receiving information about online safety incidents. The Safeguarding Governor has regular meetings with the Designated Safeguarding Lead and through these meetings appropriate information about online safety incidents will be shared.

Headteacher and Senior Leaders:

The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community.

Designated Safeguarding Lead:

- Takes day-to-day responsibility for online safety issues and has a leading role in establishing and reviewing the school's Online Safety Policy and any other relevant documents
- Ensures that all staff are aware of the procedures that need to be followed
- Provides training and advice for staff
- Receives and monitors reports of online safety incidents
- Is aware of the potential for serious child protection/safeguarding issues to arise from:
    - sharing of personal data
    - access to illegal/inappropriate materials
    - inappropriate online contact with adults/strangers

- potential or actual incidents of grooming
- cyber-bullying

IT Manager:

The IT Manager is responsible for ensuring that:

- The school's technical infrastructure is secure and is not open to misuse or malicious attack
- The school meets required online safety technical requirements and any Local Authority online safety policy/guidance that may apply
- Users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- The filtering policy is applied and updated on a regular basis
- 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 is regularly monitored in order that any misuse/attempted misuse can be reported to the Headteacher or Designated Safeguarding Lead for investigation, further action and/or sanctions

Teaching and support staff

Are responsible for ensuring that:

- They have read, understood, and signed the Staff ICT Acceptable Use Agreement
- They report any suspected misuse or problem to a member of the IT support team for initial investigation and subsequent escalation to the Headteacher or Designated Safeguarding Lead
- All digital communications with students and parents/carers should be on a professional level and only carried out using official school systems
- Students understand and follow the Online Safety Policy and Student ICT Acceptable Use Agreement (Appendix 3)
- 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

Students:

- Are responsible for using the school digital technology systems in accordance with the Student ICT Acceptable Use Agreement (Appendix 3)
- 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
- Are 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 the provision of online safety sessions at Essential Information Evenings, and the publication of online safety information in newsletters, on our website and via social media platforms. Parents/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

Parents/carers can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International

Education – Students

The education of students in online safety is an essential part of the school's online safety provision. Students 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 delivered in the following ways:

- A planned online safety curriculum is provided as part of Life lessons and should be regularly revisited
- Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities
- Students should be taught 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 supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making
- Students should understand the need for the Student ICT Acceptable Use Agreement and should be encouraged to adopt safe and responsible use both within and outside school
- Staff should act as good role models in their use of digital technologies, the Internet and mobile devices

In Key Stage 3 students cover the following topics in Life lessons:

- In the Year 7 'Social Media' unit we look at how to present yourself online, looking at how a digital footprint can last and the dangers of posting inappropriate content, e.g. from the perspective of any future employers. We discuss how to use social media responsibly by creating an online user guide, looking at the best ways to enjoy online content safely. We also cover the law regarding sexting
- In Year 9 we cover sexting and other online issues whilst also looking at the effects of alcohol. This is also covered in our Relationships and Sex Education (RSE) day when we look at the law regarding sex. They will look at online safety issues around sexting, as well as potential consequences legally.

In Key Stage 4 students cover the following in Life lessons

- In the Year 10 'Healthy Relationships' unit we cover the use of social media and what constitutes healthy, unhealthy and abusive relationships, with a specific focus on online activity
- In the Year 11 'Relationships' unit we cover issues around social media, specifically the sharing of explicit images and the loss of content control once posted online; the issues surrounding pornography, e.g. that it is not representative of real relationships, peer pressure, potentially abusive, studies showing potential harm to developing brains, etc.

By the **end of secondary school**, pupils will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence that carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

Education & 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:

- At the start of each academic year all staff receive updated online safety training notifications and key information regarding their own online safety as well as appropriate and responsible management of digital information
- All new staff receive online safety training as part of their induction programme, ensuring that they fully understand the school Online Safety Policy and ICT Acceptable Use Agreement
- The IT Manager will receive updates on wider West Sussex e-safety/e-Learning policies by attending West Sussex e-Learning Group meetings

Technical – Infrastructure/Equipment, Filtering and Monitoring

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. It will also need to ensure that the relevant people named in the above sections are 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
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users have clearly defined access rights to school technical systems and devices
- All users are provided with a username and secure password by IT Support. Users are responsible for the security of their username and password and will be required to change their password every six months
- Internet access is filtered for all users. Content lists are regularly updated and Internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes
- Internet filtering should ensure that children are safe from a range of inappropriate materials (Appendix 5)
- The school has provided differentiated user-level filtering, allowing different filtering levels for staff, sixth form students and all other students
- The IT Manager regularly monitors and records the activity of users on the school technical systems and users are made aware of this in the ICT Acceptable Use Agreements
- Users should report any actual/potential technical incident/security breach via the Online Fault Reporting system, or by speaking to a member of the IT Support team, who will escalate the issue to the IT Manager/Headteacher/Designated Safeguarding Lead as relevant
- 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. These are tested regularly. The school infrastructure and individual workstations are protected by up-to-date virus software
- Guest users requiring "staff"-level access (e.g. trainee teachers, supply teachers) will be granted the same access to the network as normal school staff, providing they read and agree to the Staff Acceptable Use Agreement. Such access will be time-limited and will be revoked once their visit comes to an end
- Any other guest users (e.g. visiting speakers) shall be granted student-level access for the duration of their visit
- Staff user accounts are disabled 7 days after the end of their contract expiry date
- Student user accounts are disabled 90 days after their school leaving date

Mobile Technologies, including BYOD (Bring Your Own Devices)

Mobile technology devices may be school owned/provided or personally owned and might include: smartphone, tablet, notebook, laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider Internet which may include services provided by the school, such as Remote Access, Foldr, or Outlook Web Access.

Personally-Owned Mobile Technology

Personally-owned mobile technology devices are welcome in school, whether they are owned by staff, or visitors. Such devices will be connected to a segregated wireless network which provides filtered Internet access and access to those school services which are available to users outside of school. Users must install a "SSL Certificate" on their devices to allow our web filter to filter their internet usage in school, users unwilling to do this will be unable to obtain Internet access.

All users should understand that the primary purpose of the use mobile/personal devices in a school context is educational. Our ICT Acceptable Use Agreements apply to all usage of the school computer system, even if the user is using a device they own personally.

The physical safety of the device is the responsibility of the owner – they need to take adequate care of the device, and the school cannot be held responsible for any loss or damage of the device. It is recommended that the device owner obtains appropriate insurance to cover the device in school, including full Theft and Accidental Damage.

Our Behaviour Policy sets out our expectations of students using mobile phones in school.

The school will offer limited, best-effort, technical support to users of personal devices. This will extend no further than assistance in connecting to the school network and accessing school services. Whilst the school attempts to be device agnostic and design its systems to be compatible with the vast majority of devices, some technology will remain incompatible and the user will be advised to use an alternative device. This is most likely to be the case with older, obsolete devices as maintaining a secure network sometimes comes at a cost to backwards compatibility.

School-Owned Mobile Technology

Mobile technology devices that are school owned, used exclusively in school, and run Microsoft Windows, will be treated as any other school computer – connected to the main school network, configured with standard anti-virus software, and managed using the same management tools as standard network computers.

Mobile technology devices that are school owned and used out of school, or, that don't run Microsoft Windows, will be treated as if they are personal devices.

Examining electronic devices

The headteacher, and any member of staff authorised to do so by the headteacher can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Assess how urgent the search is and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the DSL
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's co-operation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the DSL & SLT to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these

instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent/carer refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our behaviour policy

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

Imberhorne School recognises that AI has many uses to help pupils learn but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real.

Imberhorne School will treat any use of AI to bully pupils in line with our behaviour policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the school.

Data Protection

Personal data will be recorded, processed, transferred, and made available according to the Data Protection Act 2018 which states 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 will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for
- Every effort will be made to ensure that data held is accurate, up-to-date and that inaccuracies are corrected without unnecessary delay

- It has a Data Protection Policy
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
- It has appointed a Designated Data Protection Officer
- It has clear 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 policies and routines for the deletion and disposal of data

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
- Transfer data using encryption and secure password protected devices

Communications

When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored
- Users must immediately report 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. Ultimately, such incidents should be reported to the IT Manager, however this may be via a member of the pastoral team for students, or a line manager for staff. Copies of such communications should be retained as evidence
- Any digital communication between staff and students or Parents/Carers (email, social media, chat, blogs, VLE etc) 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
- Students should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies

Social Media - Protecting Professional Identity

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

- Ensuring that personal information is not published
- Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions

School staff should ensure that:

- On personal accounts no reference should be made in social media to students, Parents/Carers or other 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 or misappropriation of personal information

Official school social media accounts:

- Are linked to a school-owned email account
- Have login details know by more than one person (at least the Website Manager and IT Manager)
- Where possible, to enable proactive monitoring, have "post" email notifications turned on and sent to:
  - Website Manager
  - IT Support
  - Headteacher
- Will be used to celebrate student achievement, promote school activities, and general communications about school-related business
- Inappropriate posts made by parents, students, or members of the public will be hidden/removed and responded to off the social media platform concerned
- The number of staff with access to post on social media accounts will be kept to the minimum, but will include:
  - Website Manager
  - IT Manager
  - Headteacher
  - Deputy Headteachers
  - Senior Assistant Headteachers

  This will enable messages to be posted in emergency situations as well enable rapid response in the case of inappropriate postings
- Staff with access to school social media accounts are expected to act professionally, and uphold the reputation of the school at all times

Personal use:

- Personal communications are those made via personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken

Monitoring of public social media:

- As part of active social media engagement, it is considered good practice to proactively monitor the Internet for public postings about the school
- The school effectively responds to social media comments made by others as appropriate

Monitoring of students' social media/electronic devices

- See Appendix 6 – misuse of texts and images

Use of Webcams in Lessons

Webcams are not routinely used in the school but may, in particular circumstances, be a useful tool for exchanging information and supporting certain types of learning. Having a webcam in lessons will be a voluntary act by members of staff - there is no expectation that a webcam can be located in any classroom in the school without prior discussion and agreement from the Headteacher.

The webcam should **not** be positioned in a way that it will film students, its sole use is to allow access to taught material. Webcams should therefore be positioned at the front of the classroom,

facing the board. The only images available should be the teacher and any taught material visible at the front of the classroom.

Students and staff should be made aware of the location of a webcam and what it is being used for - teachers will therefore have to make it clear to students that a webcam is in operation during the lesson.

The host will announce that the call will be recorded before any recording commences so all participants are aware of the recording. In lessons involving webcams Teachers will be expected to teach lessons as normal. In most cases this will mean that teaching staff move around the classroom and may talk from different areas in the classroom. Such interaction is unlikely to appear on the webcam and may not always be audible.

If webcam footage is transmitted it will be via Google Meet, or a similar platform which restricts access to a known individual or group. Webcam footage must never be made publically available. Lessons must **only** be accessed by a student at the school.

At all times the member of staff teaching a lesson will be in full control of the webcam and will be able to terminate its use immediately if required. Potential reasons for this include:

- Change of heart by a member of staff
- Adverse impact on lessons - either through the behaviour of classes or by affecting confidence of a member of staff
- A person, other than the intended recipient of the footage, accessing taught material in lessons via the webcam
- There is criticism/negative feedback about lessons or the content of lessons

If a student is using the webcam to access lessons and is unsure about information or material being taught they can either ask a question via the webcam, or seek clarification from the teacher when appropriate.

Footage must not be recorded and saved unless such recording is initiated by the member of staff delivering the lesson. Any recorded footage may only be published by that member of staff.

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

Appendices

Appendix 1 – Illegal incidents

Appendix 2 – Other incidents

Appendix 3 – Student ICT Acceptable Use Agreement

Appendix 4 – Staff ICT Acceptable Use Policy

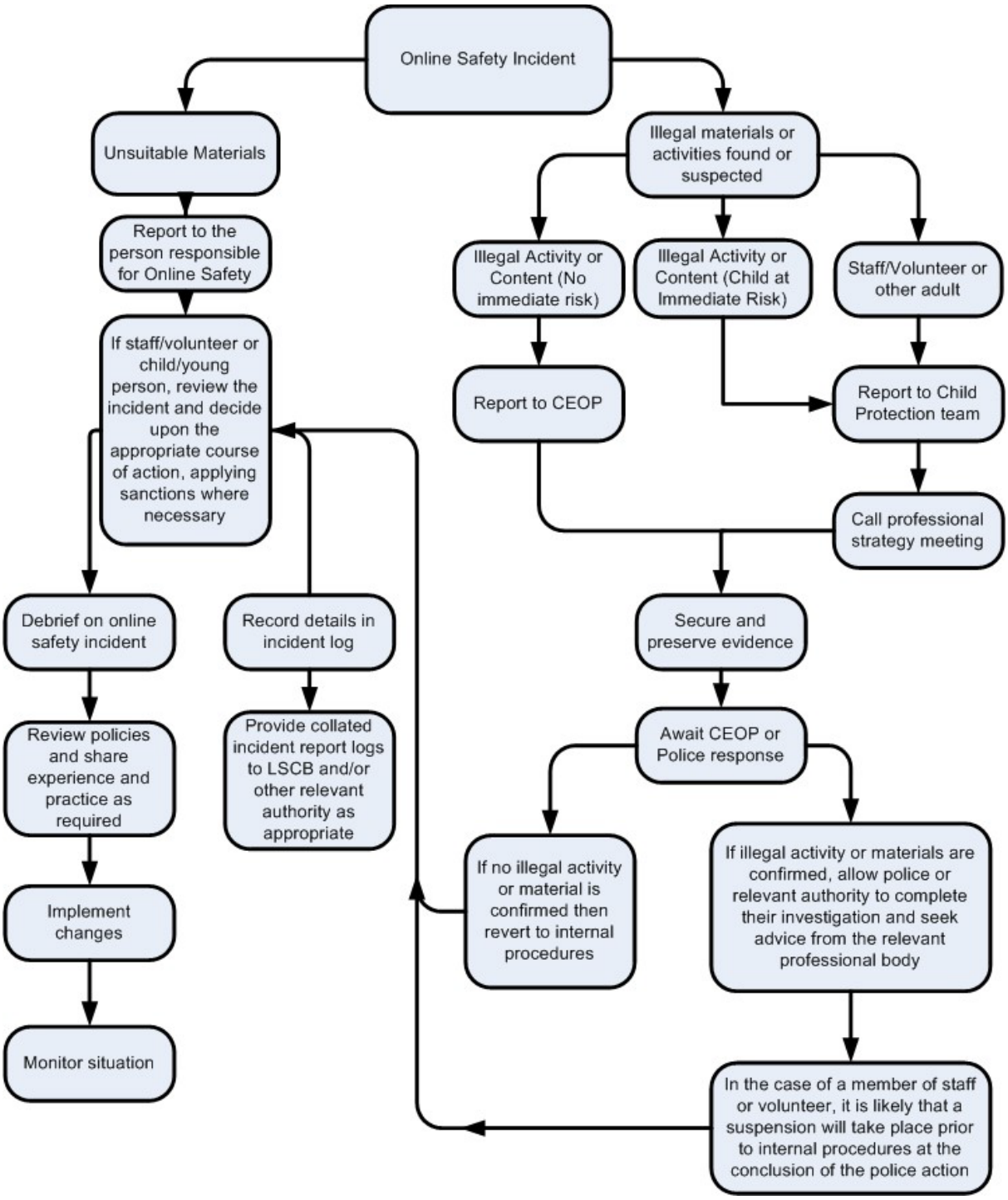
Appendix 5 - Filtered content

Appendix 6 – Misuse of texts and other images

Appendix 1 - Illegal Incidents

NB: This is a high-level flowchart based upon advice provided by SWGfL, outlining the process to be followed by our Senior Leadership team in event of an eSafety incident that breaks the law.

If there is any suspicion that the website(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) for responding to online safety incidents and report immediately to the police.



Appendix 2 - Other Incidents

In the event of suspected misuse all steps in this procedure should be followed:

- Conduct the investigation 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.
- Once this has been completed and fully investigated the school 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 disciplinary procedures implemented
    - involvement by Local Authority or national/local organisation (as relevant) o 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 or by a child
- adult material which potentially breaches the Obscene Publications Act o criminally racist material o promotion of terrorism or extremism o other criminal conduct, activity or materials

Isolate the computer or device 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 safeguarding purposes.

Appendix 3 – Student ICT Acceptable Use Agreement

As an Imberhorne student:
…I agree:

- To keep my password secret, changing it if I think someone else knows it
- To access only my own account
- Never to allow another student or member of staff to use my account
- Not to introduce unauthorised software to the school computer system, or download programs or games from the Internet
- Not to use the internet, or e-mail, in lessons unless directed to do so by my teacher
- To use my own personal technology appropriately and responsibly as directed by my teacher
- Not to play internet games at any time in school, unless they are educational and I have been given permission to do so by a teacher
- Not to use web-based e-mail (such as Hotmail), internet chat, or social networking sites (such as Facebook) while at school
- To be polite and responsible when using the school email service
- Not to send personal information about myself or others using a computer unless directed by staff
- Not to buy things over the Internet in school
- Not to create, send, or publish any material that is likely to upset others
- To treat all computer equipment with the greatest care and respect
- Not to enter ICT rooms without a member of staff
- Not to interfere with another student's computer or work
- To report any misuse, or security breach, of the school computer system to a member of the IT Support Team as soon as possible
- To report any inappropriate content I find on the internet to a member of the IT Support Team immediately, and not to share it with others
- To use the computers only for school work

… I understand that:

- All IT rooms are quiet areas and neither food nor drink is permitted in them
- It is a good idea to save my work regularly so I have less chance of it being lost
- Using file names that describe my work will help me find it again. Organising my work into folders will make this even easier
- If I break this agreement my account may be disabled or I may be banned from the internet. If appropriate, I may receive other punishments up to, and including, permanent exclusion
- All computers are regularly monitored and details of websites I visit are recorded
- I cannot access all websites in school. Certain sites are blocked by our web filter
- I shall be held responsible for all activity on my account
- These rules also apply if I log on to the school system from home using Remote Access

As a parent I understand that:

- Although Internet access in school is filtered, I will not hold the school or County Council responsible for inappropriate material that my child may obtain
- The school may use photographs or video footage of students on our website, our social media pages, around the school, and in school publications
- Great care will be taken by the school to ensure that photos or videos of students on the school website or our social media pages do not identify who they are and consequently expose them to unnecessary risk

IMBERHORNE SCHOOL Appendix 4 – Staff ICT Acceptable Use Policy

Information and Communications Technology
Staff Acceptable Use Policy

Access to the school network, including Internet access, is available to staff for educational purposes, subject to the conditions laid down in this policy.

I agree:

- To keep my password secret
- To access only my own account, and to never allow anyone else to use my account
- To use a strong password (i.e. at least 6 characters, preferably one of which is non-alphabetic)
- To change my password immediately if I suspect that someone else knows it
- To change my password to a different password when prompted by the system, and to avoid re-using the same password within a twelve month period.
- Not to store any passwords associated with school or County Council based systems as part of an automatic logon sequence, such as saving my school password in my web browser so it logs on to Remote Access automatically.
- To lock my computer, or log off, before leaving it unattended
- To log off any unattended computer I find left logged in regardless of whether I wish to use the computer
- To take steps to ensure that confidentiality of student data is maintained, such as minimising SIMS when talking to a student at my desk, and not taking electronic registers on a PC that is displaying its output on a projector.
- Not to introduce software to the school computer system without consultation with IT Support, including downloading programs from the internet.
- Not to create, transmit, display, or publish any material which is likely to cause offence, inconvenience, or needless anxiety, or is in any way defamatory. (Forwarding joke e-mails is best avoided for this reason.)
- Not to transmit "junk" or "spam" e-mail messages to others – e-mails to a large number of people unrelated to school business.
- Not to visit, or attempt to visit, websites that might be deemed to be inappropriate.
- To use only digital material which I have the copyright holders permission to use – just because I can use it, doesn't mean I should.
- Not to share personal digital contact details (such as my personal e-mail account, MSN Messenger username, personal mobile phone number) with students, nor to initiate contact with students from any personal accounts or telephones, without the explicit agreement of the Senior Management Team.
- To only enter into electronic dialogue with students within "clear and explicit professional boundaries" – i.e. only from my school e-mail account, or using school provided systems such as Wordpress or Moodle.

- It is inappropriate for me to accept students as "friends" on social networking websites such as Facebook, and that the risks of even perfectly innocent exchanges being misinterpreted from this kind of contact would leave me exposed to an unnecessarily high risk of allegations of misconduct.

- To verify that digital content I wish to use in lessons is appropriate and accessible in school, prior to the lesson concerned.

- If I use personal digital cameras, phones, or camcorders to record school events that images will be downloaded onto the school network and deleted from my device as soon as possible, and that such images will not be stored on my own computer

- If I am involved in processing credit or debit card transactions: o I must not store any card details, electronically or otherwise
    - I will only process chip and pin authorised cardholder present transactions, or those where the cardholder has processed the transaction themselves using an online service such as ParentPay
    - I will store any printed transactions receipts securely and will destroy before disposing o I will not allow anyone else to process card transactions in a manner other than that described above

IMBERHORNE SCHOOL

Information and Communications Technology
Staff Acceptable Use Policy

I understand that:

- E-mail is insecure and not guaranteed to be private, it should be used appropriately and may be monitored if misuse is suspected

- When publishing photographs of students (be it on the internet, the press, school publications, or other media) individual students must not be identifiable by name. Care should be taken that any accompanying article does not inadvertently identify students using phrases such as "third from left" or "the amazing goalkeeper".

- Published photographs of students must depict students dressed appropriately and must not cause upset, distress, or embarrassment. Care must be taken to check photographs carefully before they are made available for wider viewing on the school system.

- Photographs of students may not be published if parental consent has been refused.

- All computer systems are regularly monitored, and details of website I visit recorded, to ensure proper usage

- The computer system is intended for educational purposes and may only be used for legal activities consistent with the rules of the school.

- Any electronic "nicknames" that may be viewed by students (including the Bluetooth name of my mobile phone) should be appropriate to the school environment.

- It is preferable that any Bluetooth capability of my mobile phone is either switched off or set to hidden in school to prevent students accessing content on it.

- Personal Data as defined by the Data Protection Act – data that may identify a living, named, individual, such as student names and grades, and staff details - must not leave the school system. This means I must not copy such data to memory sticks, laptops, nor my computer at home, although I may use my computer at home to edit such data if connected to Remote Access.

- If my role requires me to share Personal Data with other agencies I must not transmit this information via standard e-mail, courier, or postal services, without first encrypting it. (Systems designed for this purpose, such as WebXchange, S2S and AnyComms meet this requirement)

- Any expression of a personal view, about the school, or County Council matters, in any form of electronic communication must be endorsed to that effect.

- I must not add any device to the credit card processing network without the explicit written approval of the IT Manager

- This agreement covers all use of the school computer system, whether in school, or from another location using Remote Access.

- Under the School's agreements with certain software companies, in particular Microsoft and Adobe, I am licensed to run prescribed software packages at home solely for school related business. I may not use such software for any other purpose, in particular any other commercial activities. Should I leave employment at

Imberhorne, these licence rights will terminate immediately, and I must uninstall such software from any computer where I have it installed.

- Failure to abide by this agreement may lead to the full or partial withdrawal of my access to the system, retrospective investigation into my use of the system, and/or disciplinary action. In some instances breaches may lead to criminal or civil prosecution.

Please report any inappropriate internet content you come across in school to a member of the IT Support team immediately. Any suspected misuse or security breach of the school computer system must also be reported to the IT Support team as soon as possible.

I have read the acceptable use policy above and agree that my usage of the school computer system will conform with the terms laid out therein:

Signed:	Print Name:	Date:

Last Updated: 01/12/11

Appendix 5 – Filtered content

All internet access in school is filtered by our Smoothwall web filtering appliance for both staff and students. This performs both category based filtering and content based filtering.

Every website is assigned a category by Smoothwall (the supplier of the filter), and an initial decision on whether to allow the page or not is taken based on whether the category is configured to be allowed.

After the initial category filtering content analysis is then performed and a second decision whether to allow the page is taken based on whether particular keywords appear on the page. In this way an article on say, pornography (disallowed), on the BBC News page (allowed) will be blocked because of its content.

From time to time there is a requirement to access a site in a category that is blocked, or that contains content that would block it – for example the pornography article on BBC News in the example above might be suitable for a Personal Development issue – being on the BBC News site it is likely to discuss pornography whilst not containing porno graphic content.

The IT Manager will make such decisions day to day if allowing the site doesn't fundamentally alter the filtering policy. Significant Filtering Policy changes will only be made following discussion with the Headteacher, and possibly wider Senior Leadership Team, depending on the gravity of the change.

We operate three different levels of filtering: Staff, KS3 & KS4 Students, and Sixth Form (KS5) Students.

The aims of our web filtering are:

- To prevent students & staff accessing illegal content
- To protect students & staff from inappropriate material
- To comply with our legal obligations (such as Prevent)
- To protect the security of our network

Category Based Web Filtering Policy

⦸ = Blocked ✓ = Allowed

Category Group	Category	Staff	KS3/4	KS5
Legal & Liability Issues	Child Abuse	⦸	⦸	⦸
	Drugs	✓	⦸	⦸
	Intolerance	⦸	⦸	⦸
	Privacy and Copyright Infringement	⦸	⦸	⦸
	Pornography	⦸	⦸	⦸
	Self Harm	⦸	⦸	⦸
	Terrorism	⦸	⦸	⦸
	Violence	⦸	⦸	⦸
Adult Themes	Abortion	✓	✓	✓
	Adult Entertainers	✓	⦸	⦸
	Adult Sites	⦸	⦸	⦸
	Alcohol and Tobacco	✓	⦸	⦸
	Body Piercing and Tattoos	✓	✓	✓

	Criminal Activity	⊘	⊘	⊘
	Fireworks	✓	✓	✓
	Gambling	⊘	⊘	⊘
	Gore	⊘	⊘	⊘
	Inappropriate/Vulgar Search Terms	✓	✓	✓
	Naturism and Nudism	⊘	⊘	⊘
	Non-pornographic Nudity	⊘	⊘	⊘
	Provocative Images	✓	✓	✓
	Restricted to Adults	⊘	⊘	⊘
	Sexuality Sites	✓	⊘	⊘
Weapons	Hunting and Sporting	⊘	⊘	⊘
	Military	✓	✓	✓
	Personal Weapons	✓	⊘	⊘
Business and Corporate	Business and Corporate	✓	✓	✓
	Charity and Non-Profit	✓	✓	✓
	Government	✓	✓	✓
	Travel and Transport Services	✓	✓	✓
Entertainment	Books	✓	✓	✓
	Celebrity	✓	✓	✓
	Computer Games	✓	⊘	⊘
	Desktop Customisation	⊘	⊘	⊘
	Graphic Novels	✓	✓	✓
	Jokes and Humour	⊘	⊘	⊘
	Magazines	✓	✓	✓
	Movies and Film	✓	✓	✓
	Museums and Art Galleries	✓	✓	✓
	Music	✓	✓	✓
	Online Games	⊘	⊘	⊘
	Radio and TV	✓	✓	✓
	Sport	✓	✓	✓
File and Image Hosting	File Hosting	✓	⊘	⊘
	Image Hosting: Moderated	✓	✓	✓
	Image Hosting: Unmoderated	⊘	⊘	⊘
File Types	"In-page" Executables	✓	✓	✓
	Archive Filetypes	✓	✓	✓
	Audio Filetypes	✓	✓	✓
	Bandwidth Wasting Filetypes	✓	✓	✓
	Document Macros	✓	✓	✓
	Executable Files	✓	✓	✓
	Instant Messaging MIME Types	✓	✓	✓
	Octect Streams	✓	✓	✓
	Safe Content Filetypes	✓	✓	✓
	Vector Graphic Filetypes	✓	✓	✓
	Video Filetypes	✓	✓	✓
	Web Content	✓	✓	✓

Finance	Cryptocurrency	✓	✓	✓
	Financial Services	✓	✓	✓
	Online Banking	✓	✓	✓

	Payday Loans	⊘	⊘	⊘
Information and Reference	Academic Institutions	✓	✓	✓
	Education and Reference	✓	✓	✓
	Mapping	✓	✓	✓
	News	✓	✓	✓
	Plagiarism	✓	⊘	⊘
	Sex Education	✓	✓	✓
	Translation	✓	⊘	⊘
	Weather	✓	✓	✓
	Wikipedia: Editing	✓	⊘	⊘
IT & Technical	Collaboration Software	✓	✓	✓
	Computing	✓	✓	✓
	Games Consoles	✓	✓	✓
	Microsoft Office 365	✓	✓	✓
	ClassDojo App	✓	✓	✓
	Facebook App [1]	✓	✓	✓
	Instagram App [1]	✓	✓	✓
	Snapchat App [1]	✓	✓	✓
	Twitter App [1]	✓	✓	✓
	Mobile/Cell Phones	✓	✓	✓
	Peer-to-peer Networking	⊘	⊘	⊘
	Remote Desktop	✓	⊘	⊘
	AEM Web Portal	✓	✓	✓
	GoTo Software Suite	✓	✓	✓
	Hudl App	✓	✓	✓
	Skype	✓	✓	✓
	Zoom	✓	✓	✓
	Web Hosting	✓	✓	✓
	Webmail	✓	⊘	⊘
Lifestyle	Clothing & Accessories	✓	✓	✓
	Food and Dining	✓	✓	✓
	Gardening	✓	✓	✓
	Online Auctions	✓	⊘	⊘
	Online Shopping	✓	✓	✓
	Parenting and Baby	✓	✓	✓
	Pets	✓	✓	✓
	Real Estate and Property	✓	✓	✓
	Religion	✓	✓	✓
	Time-wasting	✓	⊘	⊘
	Toys and Games	✓	✓	✓
	Vacations	✓	✓	✓
	Vehicles and Motoring	✓	✓	✓
	Wedding	✓	✓	✓
Malware & Hacking	Hacking	✓	⊘	⊘
	Internationalised Domain Names	✓	✓	✓
	Malware and Phishing	⊘	⊘	⊘
	Web Proxies	⊘	⊘	⊘
Medical	Medical Information	✓	✓	✓

Multimedia	Amazon Prime	✓	✓	✓
	Audio and Video	✓	✓	✓
	BBC iPlayer	✓	✓	✓
	iTunes	✓	✓	✓
	Live Streaming	✓	✓	✓
	Netflix	⊘	⊘	⊘
	YouTube	✓	✓ (2)	✓ (2)
	YouTube HD streaming	✓	✓ (2)	✓ (2)
Search Engines	Google Instant Previews	✓	✓	✓
	Google Link Redirector	✓	✓	✓
	Image Search	✓	✓	✓
	Job Search	✓	✓	✓
	Question & Answer	✓	✓	✓
	Reverse Image Search	✓	✓	✓
	Search Suggestions	✓	✓	✓
	Secure Search	✓	✓	✓
	Web Search	✓	✓	✓
Social Media	Blogs	✓	⊘	⊘
	Dating and Companionship Sites	⊘	⊘	⊘
	Discussion Forums	✓	⊘	⊘
	Facebook	✓	⊘	⊘
	Facebook: Posts & Updates	⊘	⊘	⊘
	Instant Messaging, VoIP and Web Conferencing	⊘	⊘	⊘
	Social Networking Sites	⊘	⊘	⊘
	Twitter: Updates	✓	⊘	⊘
Web Infrastructure	Adverts	⊘	⊘	⊘
	APIs & Web Libraries	✓	✓	✓
	Connect for Chromebooks	✓	✓	✓
	Content Delivery	✓	✓	✓
	Internet Speed Tests	✓	✓	✓
	Parked Domains	⊘	⊘	⊘
	Smoothwall Products	✓	✓	✓
	Software Updates	✓	✓	✓
	SSL / CRL	✓	✓	✓
	Transparent HTTPS Incompatible Sites	✓	✓	✓
	URL Shortening	✓	✓	✓
	User Tracking & Site Stats	✓	✓	✓

Notes:

1) These social media apps are allowed, even though their web-based cousins are blocked, to encourage students to keep their mobile devices on the school WiFi. Blocking these apps gives students the impression the wireless is broken and then they hop off onto their mobile data and get no filtering whatsoever.

2) KS3/4 Students have YouTube's Restricted Mode forcibly enabled, KS5 Students get unrestricted access. Restricted Mode hides videos YouTube deem unsuitable for younger audiences based on decisions made by YouTube's moderators and algorithms.

Appendix 6 – Misuse of texts and images

Information for Students and Parents/Carers

We are very proud to embrace the rapid progress made in communication technology within recent years. This has brought countless benefits to our students as they become more independent thinkers and researchers. Whilst any new technology brings opportunities it also brings the risk of misuse. This brief document aims to inform you of some of the 'misuse' issues schools are faced with and the stance we take as they arise. The issues of most concern nationally, are 'sexting' and 'bullying videos or social media activity'.

We have information about online safety on our website and suggest that parents and/or students access some of this advice alongside any action taken by the school.

Where the school suspects that a student has inappropriate material on an electronic device, the school has the right to examine such a device. Department for Education guidance states: 'Where the person conducting the search finds an electronic device that is prohibited by the school rules or that they reasonably suspects has been, or is likely to be, used to commit an offence or cause personal injury or damage to property, they may examine any data or files on the device where there is a good reason to do so. They may also delete data or files if they think there is a good reason to do so, unless they are going to give the device to the police. This power applies to all schools and there is no need to have parental consent to search through a young person's mobile phone if it has been seized in a lawful 'without consent' search and is prohibited by the school rules or is reasonably suspected of being, or being likely to be, used to commit an offence or cause personal injury or damage to property.' *Searching, screening and confiscation: Advice for Headteachers, School Staff and Governing Bodies* (January 2018)

What is sexting and catfishing?

Sexting is the act of sending sexually explicit messages, photos or videos electronically, primarily between mobile phones.
Catfishing is the act of creating a fake online identity to deceive others, often for romantic or financial gain.

What are bullying videos?

It is an offence to disclose a private photo or video without the consent of an individual who appeared in the photo or video, with the intention of causing that individual distress.

Why do people do it?

People sext to show off, to entice someone (who may be much younger), to show interest in someone, or to prove commitment. Problems can also happen when relationships end and someone is left in possession of highly compromising materials. This can lead to such images being posted maliciously onto the internet without the subject's consent.

Why is sexting and catfishing dangerous?

Once a photo or video is sent, control of that image or video is lost, and it is impossible to take it back. The person receiving it can forward the image or video, copy it, post it online, or share it with anyone. In addition to the emotional damage that can come from having a sexual image shared with an entire school or community, there is damage to the reputation and self-esteem of that person. Remember that once that photo or video is out there, it's impossible to take it back and you would be amazed how quickly images and videos spread.

There are also very serious legal consequences. Sharing sexual or naked photos or videos of minors, even sharing with other minors, is **illegal**. Sexting can and has led to prosecution for child pornography and the offender being placed on the sex offenders register. Even a minor sexting an image of him/her is breaking the law.

What happens when we come across cases of 'Sexting', 'catfishing', or 'Bullying videos and social media activity'?
Although we judge each case individually, it is highly likely that any student found to have distributed images or videos of a sexual or bullying nature to others, will be given a **Fixed Term Exclusion**. We would take an equally firm stance against students requesting images or videos from other students.

What advice do we give to our students?
Respect yourself and others. Don't ask people for sexual pictures or videos, and if asked, don't provide them.

Remember: Stop. Block. Tell.

- Refuse to pass along sexting messages
- Tell friends to stop sexting and block communication with friends who send sexting messages
- If you know someone is sending sexually revealing photos or videos or someone has them, you should tell an adult immediately and report it to the hosting website

Take care of your friends.
If you know your friends are sending or receiving sexually explicit photos, videos or messages, tell them to stop. Let them know that there are serious and dangerous consequences and that it's just not worth it. If you feel they are being pressured into this… tell an adult IMMEDIATELY!

Misuse of images, videos and text of a non-sexual nature.
Pictures or videos of a student (or adult employee in a school) may be posted on to social media sites such as 'Facebook', 'twitter' or 'YouTube' without their permission. These sites can give viewers the opportunity to make comments which are often derogatory and hurtful for the subject(s) of the post… even if that was not the original intention of the person uploading the image. We would also seek to support any student who has been the victim of hurtful text comments via social media sites, email or mobile phone.

Context
Inappropriate interactions that involve students and have an impact on a student's wellbeing or welfare will be dealt with regardless of whether they originate in school or beyond school.

How does Imberhorne School react to such cases?
Each case is judged on its individual merit. However, a student who has knowingly taken a picture/video clip of another student/adult and posted or shared this image, without permission, is likely to be issued with a sanction ranging from internal isolation to fixed term exclusion. We would also take a similarly punitive stance in support of any student who had become the victim of hurtful comments posted on social media sites such as 'Facebook'. This would apply whether the victim had been contacted directly or simply shown the messages via a third party. We would urge the victim to keep records of such instances, whenever possible, and contact his/her Head of Year as soon possible for further advice and support.

Conclusion
The information contained within this document forms part of our wider commitment to safeguarding and positive behaviour. We would like all of our students to ensure that their actions never cause hurt or humiliation to others. We would urge Parents/Carers to ensure that their children fully understand both the need to use technology responsibly and respectfully, and the consequences that follow if such advice is not taken.