

RIVERSIDE SCHOOL



Online Safety Policy

APPROVED BY GOVERNORS

RESPONSIBLE PERSON – HEADTEACHER

Contents

Statement of Intent

1. [Legal Framework](#)
2. [Roles and Responsibilities](#)
3. [Managing Online Safety](#)
4. [Cyberbullying](#)
5. [Child-on-Child Sexual Abuse and Harassment](#)
6. [Grooming and Exploitation](#)
7. [Mental Health](#)
8. [Online Hoaxes and Harmful Online Challenges](#)
9. [Cyber Crime](#)
10. [Online Safety Training for Staff](#)
11. [Online Safety and the Curriculum](#)
12. [Use of Technology in the Classroom](#)
13. [Use of Smart Technology](#)
14. [Educating Parents](#)
15. [Internet Access](#)
16. [Filtering and Monitoring Online Activity](#)
17. [Network Security](#)
18. [Emails](#)
19. [Generative Artificial Intelligence \(AI\)](#)
20. [Social Networking](#)
21. [The School Website](#)
22. [Use of Devices](#)
23. [Monitoring and Review](#)

[Appendix 1 – Acceptable Use Agreement \(Staff\)](#)

[Appendix 2 – Acceptable Use Agreement \(Pupils\)](#)

[Appendix 3 – Acceptable Use Agreement Including Photo/ Video Permissions \(Parents/ Carers\)](#)

[Appendix 4 – Protocol for Responding to Online Safety Infringements](#)

Statement of Intent

Riverside School understands that using online services is an important aspect of raising educational standards, promoting pupil achievement, and enhancing teaching and learning. The use of online services is embedded throughout the school; therefore, there are a number of controls in place to ensure the safety of pupils and staff.

The breadth of issues classified within online safety is considerable, but they can be categorised into four areas of risk:

- **Content:** Being exposed to illegal, inappropriate or harmful material e.g., pornography, racism, misogyny, anti-Semitism, radicalisation, disinformation (including fake news), conspiracy theories, self-harm and suicide and discriminatory or extremist views.
- **Contact:** Being subjected to harmful online interaction with other users e.g., peer pressure, commercial advertising, and adults posing as children or young adults with the intention to groom or exploit children for sexual, criminal, financial or other purposes.
- **Conduct:** Personal online behaviour that increases the likelihood of, or causes harm e.g., sending and receiving explicit messages and images, and non-consensual sharing of nudes and semi-nudes and/ or pornography, sharing other explicit images and cyberbullying.
- **Commerce:** Risks such as online gambling, inappropriate advertising, phishing and/ or financial scams.

The measures implemented to protect pupils and staff revolve around these areas of risk. Our school has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff.

1. Legal Framework

This policy has due regard to all relevant legislation and statutory guidance including, but not limited to, the following:

- Online Safety Act 2023
- Voyeurism (Offences) Act 2019
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- DfE 'Filtering and monitoring standards for schools and colleges'
- DfE 'Harmful online challenges and online hoaxes'
- DfE 'Keeping Children Safe in Education 2025'
- DfE 'Teaching online safety in school'
- DfE 'Searching, screening and confiscation'
- DfE 'Generative artificial intelligence in education'
- Department for Digital, Culture, Media and Sport and UK Council for Internet Safety 'Sharing nudes and semi-nudes: advice for education settings working with

children and young people'

- UK Council for Child Internet Safety 'Education for a Connected World – 2020 edition'
- National Cyber Security Centre 'Small Business Guide: Cyber Security'

This policy operates in conjunction with the following school policies:

- Social Media Policy
- Allegations of Abuse Against Staff Policy
- Technology Acceptable Use Agreement
- Cyber Security Policy
- Cyber Response and Recovery Plan
- Safeguarding Policy
- Anti-Bullying Policy
- Staff Code of Conduct
- Regulation Support Policy
- Disciplinary Policy and Procedure for Staff
- Data Protection Policy
- Data Breach Policy
- Acceptable Use Agreement for Staff (see Appendix 1)
- Acceptable Use Agreement for Pupils (see Appendix 2)
- Acceptable Use Agreement Including Photo/ Video Permissions (Parents) (see Appendix 3)
- Protocol for Responding to Online Safety Infringements (see Appendix 4)

2. Roles and Responsibilities

The governing board will be responsible for:

- Ensuring that this policy is effective and complies with relevant laws and statutory guidance.
- Ensuring the designated safeguarding lead's (DSL) remit covers online safety.
- Reviewing this policy on an annual basis.
- Ensuring their own knowledge of online safety issues is up to date.
- Ensuring all staff undergo safeguarding and child protection training, including online safety, at induction and at regular intervals.
- Ensuring that there are appropriate filtering and monitoring systems in place.
- Ensuring that the effectiveness of filtering and monitoring systems is reviewed at least annually in liaison with ICT staff and service providers.
- Ensuring that the SLT and other relevant staff have an awareness and understanding of the filtering and monitoring provisions in place, and manage them effectively and know how to escalate concerns when identified.
- Ensuring that all relevant school policies have an effective approach to planning for, and responding to, online challenges and hoaxes embedded within them.
- Ensuring compliance with the DfE's 'Meeting digital and technology standards in schools and colleges', with particular regard to the filtering and monitoring

standards in relation to safeguarding.

The headteacher will be responsible for:

- Ensuring that online safety is a running and interrelated theme throughout the school's policies and procedures, including in those related to the curriculum, teacher training and safeguarding.
- Supporting the DSL and the deputy DSL by ensuring they have enough time and resources to carry out their responsibilities in relation to online safety.
- Ensuring staff receive regular, up to date and appropriate online safety training and information as part of their induction and safeguarding training.
- Ensuring online safety practices are audited and evaluated.
- Organising engagement with parents to keep them up to date with current online safety issues and how the school is keeping pupils safe.
- Working with the DSL and administration and data manager to conduct regular light-touch reviews of this policy.
- Working with the DSL, administration and data manager and governing board to update this policy on an annual basis.
- Identifying and assigning roles and responsibilities to manage the school's filtering and monitoring systems.
- Appointing an SLT digital lead in line with the Cyber Security Policy. At Riverside School this will be the DSL.

The DSL will be responsible for:

- Taking the lead responsibility for online safety in the school.
- Undertaking training so they understand the risks associated with online safety and can recognise additional risks that pupils with SEND face online.
- Liaising with relevant members of staff on online safety matters e.g., the administration and data manager and ICT technicians.
- Ensuring online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented.
- Ensuring safeguarding is considered in the school's approach to remote learning.
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by pupils and staff, and ensuring all members of the school community understand this procedure.
- Understanding the filtering and monitoring processes in place at the school.
- Ensuring that all safeguarding training given to staff includes an understanding of the expectations, roles and responsibilities in relation to filtering and monitoring systems at the school.
- Maintaining records of reported online safety concerns as well as the actions taken in response to concerns.
- Monitoring online safety incidents to identify trends and any gaps in the school's provision and using this data to update the school's procedures.
- Reporting to the governing board about online safety on a regular basis.
- Working with the headteacher, administration and data manager and ICT

technicians to conduct regular light-touch reviews of this policy.

- Working with the headteacher and governing board to update this policy on an annual basis.

ICT technicians will be responsible for:

- Providing technical support in the development and implementation of the school's online safety policies and procedures.
- Implementing appropriate security measures as directed by the headteacher and those with delegated responsibilities.
- Ensuring that the school's filtering and monitoring systems are updated as appropriate.
- Working with the DSL and administration and data manager to conduct regular light-touch reviews of this policy.

The administration and data manager will be responsible for:

- Supervising and directing the work of the ICT technicians.
- Reporting any online safety related issues that arise to the headteacher and DSL.
- Ensuring that users may only access the school's networks through an authorised and properly enforced password protection policy.
- Ensuring that provision exists for misuse and malicious attack e.g., keeping virus protection up to date.
- Ensuring the security of the school's ICT system.
- Ensuring the access controls/ encryption exists to protect personal and sensitive information held on school owned devices.
- Ensuring the school's policy on web filtering is applied and updated on a regular basis.
- Ensuring LGfL are informed of issues relating to the filtering applied by the grid.
- Keeping up to date with the school's Online Safety Policy and technical information in order to ensure ICT technicians effectively carry out their roles and to inform and update others as relevant.
- Ensuring ICT use is regularly monitored in order that any misuse/ attempted misuse can be investigated.
- Ensuring appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster.
- Keeping documentation of the school's online security and technical procedures updated.
- Ensuring that all data held has appropriate access controls in place.

All staff members will be responsible for:

- Taking responsibility for the security of ICT systems and electronic data they use or have access to.
- Modelling good online behaviours.
- Maintaining a professional level of conduct in their personal use of technology.

- Having an awareness of online safety issues.
- Ensuring they are familiar with, and understand, the indicators that pupils may be unsafe online.
- Reporting concerns in line with the school's reporting procedure.
- Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum.

Pupils will be responsible for:

- Adhering to the Acceptable Use Agreement and other relevant policies.
- Seeking help from school staff if they are concerned about something they or a peer have experienced online.
- Reporting online safety incidents and concerns in line with the procedures within this policy.

Parents/ Carers will be responsible for:

- Supporting the school in promoting online safety and endorsing the Acceptable Use Agreement, which includes the pupils' use of the internet and the school's use of photographic and video images.
- Reading, understanding and promoting the school's online safety form.
- Accessing the school website/ online pupil/ pupil records in accordance with the relevant school acceptable use agreement.
- Consulting with the school if they have any concerns about their children's use of technology.

External groups are responsible for:

- Any external individual/ organisation will sign an Acceptable Use Agreement prior to using any equipment or the internet within the school.

3. Managing Online Safety

All staff will be aware that technology is a significant component in many safeguarding and wellbeing issues affecting young people, particularly owing to the rise of social media and the increased prevalence of children using the internet.

The DSL has overall responsibility for the school's approach to online safety, with support from the administration and data manager and the senior leadership team where appropriate, and will ensure that there are strong processes in place to handle any concerns about pupils' safety online. The DSL should liaise with the Police or Children's Social Care Services (CSCS) for support responding to harmful online sexual behaviour.

The importance of online safety is integrated across all school operations in the following ways:

- Staff receive regular training.
- Staff receive regular email updates regarding online safety information and any changes to online safety guidance or legislation.
- Online safety is integrated into learning throughout the curriculum.

Handling Online Safety Concerns

Any disclosures made by pupils to staff members about online abuse, harassment or exploitation, whether they are the victim or disclosing on behalf of another child, will be handled in line with the Safeguarding Policy.

Staff will be aware that harmful online sexual behaviour can progress on a continuum, and appropriate and early intervention can prevent abusive behaviour in the future. Staff will also acknowledge that pupils displaying this type of behaviour are often victims of abuse themselves and should be suitably supported.

The victim of online harmful sexual behaviour may ask for no one to be told about the abuse. The DSL will consider whether sharing details of the abuse would put the victim in a more harmful position, or whether it is necessary in order to protect them from further harm. Ultimately the DSL will balance the victim's wishes against their duty to protect the victim and other young people. The DSL and other appropriate staff members will meet with the victim's parents to discuss the safeguarding measures that are being put in place to support their child and how the report will progress.

Confidentiality will not be promised, and information may be still shared lawfully, for example, if the DSL decides that there is a legal basis under UK GDPR such as the public task basis whereby it is in the public interest to share the information. If the decision is made to report abuse to CSCS or the Police against the victim's wishes, this must be handled extremely carefully – the reasons for sharing the information should be explained to the victim and appropriate specialised support should be offered.

Concerns regarding a staff member's online behaviour are reported to the headteacher, who decides on the best course of action in line with the relevant policies. If the concern is about the headteacher, it is reported to the chair of governors.

Concerns regarding a pupil's online behaviour are reported to the DSL, who investigates concerns with relevant staff members e.g., the headteacher and ICT technicians, and manages concerns in accordance with relevant policies depending on their nature e.g., the Regulation Support Policy and Safeguarding Policy.

Where there is a concern that illegal activity has taken place, the headteacher contacts the Police.

The school avoids unnecessarily criminalising pupils e.g., calling the Police, where criminal behaviour is thought to be inadvertent and as a result of ignorance or normal developmental curiosity e.g., a pupil has taken and distributed indecent imagery of

themselves. The DSL will decide in which cases this response is appropriate and will manage such cases in line with the Safeguarding Policy.

All online safety incidents and the school's response are recorded by the DSL.

4. Cyberbullying

Cyberbullying can include, but is not limited to, the following:

- Threatening, intimidating or upsetting text messages.
- Threatening or embarrassing pictures and video clips sent via mobile phone cameras.
- Silent or abusive phone calls or using the victim's phone to harass others, to make them think the victim is responsible.
- Threatening or bullying emails, possibly sent using a pseudonym or someone else's name.
- Unpleasant messages sent via instant messaging.
- Unpleasant or defamatory information posted to blogs, personal websites and social networking sites e.g., Facebook.
- Abuse between young people in intimate relationships online i.e., teenage relationship abuse.
- Discriminatory bullying online i.e., homophobia, racism, misogyny/ misandry.

The school will be aware that certain pupils can be more at risk of abuse and/ or bullying online, such as lesbian, gay, bisexual or gender questioning pupils.

Cyberbullying against pupils or staff is not tolerated under any circumstances. Incidents of cyberbullying are dealt with quickly and effectively wherever they occur in line with the Anti-Bullying Policy.

5. Child-on-Child Sexual Abuse and Harassment

Pupils may also use the internet and technology as a vehicle for sexual abuse and harassment. Staff will understand that this abuse can occur both in and outside of school, off and online, and will remain aware that pupils are less likely to report concerning online sexual behaviours, particularly if they are using websites that they know adults will consider to be inappropriate for their age.

The following are examples of online harmful sexual behaviour of which staff will be expected to be aware:

- Threatening, facilitating or encouraging sexual violence.
- Upskirting i.e., taking a picture underneath a person's clothing without consent and with the intention of viewing their genitals, breasts or buttocks.
- Sexualised online bullying e.g., sexual jokes or taunts.
- Unwanted and unsolicited sexual comments and messages.

- Consensual or non-consensual sharing of sexualised imagery.
- Abuse between young people in intimate relationships online i.e., teenage relationship abuse.

All staff will be aware of and promote a zero-tolerance approach to sexually harassing or abusive behaviour, and any attempts to pass such behaviour off as trivial or harmless. Staff will be aware that allowing such behaviour could lead to a school culture that normalises abuse and leads to pupils becoming less likely to report such conduct.

Staff will be aware that creating, possessing and distributing indecent imagery of other children i.e., individuals under the age of 18, is a criminal offence, even where the imagery is created, possessed and distributed with the permission of the child depicted, or by the child themselves.

The school will be aware that interactions between the victim of online harmful sexual behaviour and the alleged perpetrator(s) are likely to occur over social media following the initial report, as well as interactions with other pupils taking “sides”, often leading to repeat harassment. The school will respond to these incidents in line with the Safeguarding Policy and the Social Media Policy.

The school will respond to all concerns regarding online child-on-child sexual abuse and harassment, regardless of whether the incident took place on the school premises or using school-owned equipment. Concerns regarding online child-on-child abuse will be reported to the DSL, who will investigate the matter in line with the Safeguarding Policy.

6. Grooming and Exploitation

Grooming is defined as the situation whereby an adult builds a relationship, trust and emotional connection with a child with the intention of manipulating, exploiting and/ or abusing them.

Staff will be aware that grooming often takes place online and that pupils who are being groomed are commonly unlikely to report this behaviour for many reasons e.g., the pupil may have been manipulated into feeling a strong bond with their groomer and may have feelings of loyalty, admiration or love, as well as fear, distress and confusion.

Due to the fact pupils are less likely to report grooming than other online offences, it is particularly important that staff understand the indicators of this type of abuse. The DSL will ensure that online safety training covers online abuse, the importance of looking for signs of grooming, and what the signs of online grooming are, including:

- being secretive about how they are spending their time online;
- having an older boyfriend or girlfriend, usually one that does not attend the school and whom their close friends have not met; and
- having money or new possessions e.g., clothes and technological devices, that the cannot or will not explain.

Child Sexual Exploitation (CSE) and Child Criminal Exploitation (CCE)

Although CSE often involves physical sexual abuse or violence, online elements may be prevalent e.g., sexual coercion and encouraging children to behave in sexually inappropriate ways through the internet. In some cases, a pupil may be groomed online to become involved in a wider network or exploitation e.g., the production of child pornography or forced child prostitution and sexual trafficking.

CCE is a form of exploitation in which children are forced or manipulated into committing crimes for the benefit of their abuser e.g., drug transporting, shoplifting and serious violence. While these crimes often take place in person, it is increasingly common for children to be groomed and manipulated into participating through the internet.

Where staff have any concerns about pupils with relation to CSE or CCE, they will bring these concerns to the DSL without delay, who will manage the situation in line with the Safeguarding Policy.

Radicalisation

Radicalisation is the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups. This process can occur through direct recruitment e.g., individuals in extremist groups identifying, targeting and contacting young people with the intention of involving them in terrorist activity, or by exposure to violent ideological propaganda.

Children who are targets for radicalisation are likely to be roomed by extremists online to the extent that they believe the extremist has their best interests at heart, making them more likely to adopt the same radical ideology.

Staff members will be aware of the factors which can place certain pupils at increased vulnerability to radicalisation, as outlined in the Prevent Policy. Staff will be expected to exercise vigilance towards any pupils displaying indicators that they have been, or are being, radicalised.

Where staff have a concern about a pupil relating to radicalisation, they will report this to the DSL without delay, who will handle the situation in line with the Safeguarding Policy and Prevent Policy.

7. Mental Health

Staff will be aware that online activity both in and outside of school can have a substantial impact on a pupil's mental state, both positively and negatively. The DSL will ensure that training is available to help ensure that staff members understand popular social media sites and terminology, the ways in which social media and the internet in general can impact mental health, and the indicators that a pupil is suffering from challenges in their mental health. Concerns about the mental health of a pupil will be dealt with in line with

the Regulation Support Policy. This policy should be read alongside the following key policies:

- Safeguarding Pupils Against Mobile Phones, Cameras and Smart Watch Devices Policy
- Data Protection Policy
- Cyber Security Policy
- Safeguarding Policy

8. Online Hoaxes and Harmful Online Challenges

For the purposes of this policy, an “online hoax” is defined as a deliberate lie designed to seem truthful, normally one that is intended to scaremonger or to distress individuals who come across it, spread on online social media platforms.

For the purposes of this policy, “harmful online challenges” refers to challenges that are targeted at young people and generally involve users recording themselves participating in an online challenge, distributing the video through social media channels and daring others to do the same. Although many online challenges are harmless, an online challenge becomes harmful when it could potentially put the participant at risk of harm, either directly as a result of partaking in the challenge itself or indirectly as a result of the distribution of the video online – the latter will usually depend on the age of the pupil and the way in which they are depicted in the video.

Where staff suspect there may be a harmful online challenge or online hoax circulating amongst pupils in the school, they will report this to the DSL Immediately.

The DSL will conduct a case-by-case assessment for any harmful online content brought to their attention, establishing the scale and nature of the possible risk to pupils, and whether the risk is one that is localised to the school or the local area, or whether it extends more widely across the country. Where the harmful content is prevalent mainly in the local area, the DSL will consult with the LA about whether quick local action can prevent the hoax or challenge from spreading more widely.

Prior to deciding how to respond to a harmful online challenge or hoax, the DSL and the headteacher will decide whether each proposed response is:

- In line with any advice received from a known, reliable source e.g., the UK Safer Internet Centre, when fact-checking the risk of online challenges or hoaxes.
- Careful to avoid needlessly scaring or distressing pupils.
- Not inadvertently encouraging pupils to view the hoax or challenge where they would not have otherwise come across it e.g., where consent is explained to younger pupils but is almost exclusively being shared amongst older pupils.
- Proportional to the actual or perceived risk.
- Helpful to the pupils who are, or are perceived to be, at risk.
- Appropriate for the relevant pupils’ age and developmental stage.

- Supportive.
- In line with the Safeguarding Policy.

Where the DSL's assessment finds an online challenge to be putting pupils at risk of harm, they will ensure that the challenge is directly addressed to the relevant pupils e.g., those within a particular age range that is directly affected or individual pupils at risk where appropriate.

The DSL and headteacher will only implement a school-wide approach to highlighting potential harms of a hoax or challenge when the risk of needlessly increasing pupils' exposure to the risk is considered and mitigated as far as possible.

9. Cyber Crime

Cyber crime is criminal activity committed using computers and/ or the internet. There are two key categories of cyber crime:

- Cyber enabled – these crimes can be carried out offline; however, are made easier and can be conducted at higher scales and speeds online e.g., fraud, purchasing and selling of illegal drugs, and sexual abuse and exploitation.
- Cyber dependent – these crimes can only be carried out online or by using a computer e.g., making, supplying or obtaining malware, illegal hacking, and 'booting', which means overwhelming a network, computer or website with internet traffic to render it unavailable.

The school will factor into its approach to online safety the risk that pupils with a particular affinity or skill in technology may become involved, whether deliberately or inadvertently, in cyber crime. Where there are any concerns about a pupil's use of technology and their intentions with regard to using their skill and affinity towards it, the DSL will consider a referral to the Cyber Choices Programme, which aims to intervene where children are at risk of committing cyber crime and divert them to a more positive use of their skills and interests.

The DSL and headteacher will ensure that pupils are taught, throughout the curriculum, how to use technology safely, responsibly and lawfully.

10. Online Safety Training for Staff

The DSL will ensure that all safeguarding training given to staff includes elements of online safety, including how the internet can facilitate abuse and exploitation, and understanding the expectations, roles and responsibilities relating to filtering and monitoring systems. All staff will be made aware that pupils are at risk of abuse, by their peers and by adults, online as well as in person, and that, often, abuse will take place concurrently via online channels and in daily life.

Staff training will include a specific focus on harmful online narratives such as

misinformation, disinformation, and conspiracy theories, helping staff to recognise the signs of influence or vulnerability among pupils.

Training will equip staff with the knowledge and confidence to identify signs of online harm, respond appropriately to disclosures or concerns, and support pupils in developing critical thinking skills and safe online behaviours.

Staff will also be guided on how to embed online safety themes across the wider curriculum, promoting a consistent, whole-school approach to digital safeguarding.

11. Online Safety and the Curriculum

Online safety is embedded throughout the curriculum. The school has a clear, progressive online safety education programme as part of the ICT/ PHSE curriculum. It is built on LA/ LGfL e-safeguarding and e-literacy framework for EYFS to Y6 national guidance. This covers a range of skills and behaviours appropriate to their age and experience, including:

- To STOP and THINK before you CLICK.
- To develop a range of strategies to evaluate and verify information before accepting its accuracy .
- To be aware that the author of a website page may have a particular bias or purpose and to develop skills to recognise what that may be.
- To know how to narrow down or refine a search.
- (for older pupils) to understand how search engines work and to understand that this affects the results they see at the top of the listings.
- To understand acceptable behaviour when using an online environment/ email i.e. be polite, no bad or abusive language or other inappropriate behaviour, keeping personal information private.
- To understand how photographs can be manipulated and how web content can attract the wrong sort of attention.
- To understand why online 'friends' may not be who they say they are and to understand why they should be careful in online environments.
- To understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos, and to know how to ensure they have turned on privacy settings.
- To understand why they must not post pictures or videos of others without their permission.
- To know not to download any files – such as music files – without permission.
- To have strategies for dealing with receipt of inappropriate materials.
- (for older pupils) to understand why and how some people will 'groom' young people for sexual reasons.
- To understand the impact of cyber bullying, sexting and trolling, and know how to seek help if they are affected by any form of online bullying.
- To know how to report any abuse including cyber bullying, and how to seek technologies i.e., parent or carer, teacher or trusted staff member, or an organisation such as ChildLine or the CLICK CEOP button.

The school:

- Plans internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- Will remind pupils about their responsibilities through an end-user acceptable use agreement, which every pupil will sign/ will be displayed throughout the school/ will be displayed when a pupil logs on to the school network.
- Ensures staff will model safe and responsible behaviour in their own use of technology during lessons.
- Ensures that when copying materials from the web, staff and pupils understand issues relating to plagiarism; how to check copyright and also know that they must respect and acknowledge copyright/ intellectual property rights.
- Ensures that staff and pupils understand the issues around aspects of the commercial use of the internet, as age appropriate. This may include risks of pop-ups, online purchases, online gambling and online gaming.

Online safety teaching is always appropriate to pupils' ages and developmental stages.

Pupils are taught the underpinning knowledge and behaviours that can help them to navigate the online world safely and confidently regardless of the device, platform or app they are using. The underpinning knowledge and behaviours pupils learn through the curriculum include the following:

- How to evaluate what they see online.
- How to recognise techniques used for persuasion.
- Acceptable and unacceptable online behaviour.
- How to identify online risks.
- How and when to seek support.
- Knowledge and behaviours that are covered in the government's online media literacy strategy.

The online risks pupils may face online are always considered when developing the curriculum.

The school's approach to teaching online safety in the curriculum will reflect the ever-evolving nature of online risks, ensuring pupils develop the knowledge and resilience to navigate digital spaces safely and responsibly. Online safety education will address four key categories of risk: content, contact, conduct and commerce.

Content Risks

Pupils will be taught how to critically evaluate online content and identify material that is illegal, inappropriate or harmful. The curriculum will include discussions around harmful content such as pornography, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, extremism, misinformation, disinformation (including fake news), and

conspiracy theories. Lessons will equip pupils with the skills to question sources, verify information, and understand the dangers of engaging with such content.

Contact Risks

The school will educate pupils about the potential dangers of interacting with others online. Pupils will explore topics such as peer pressure, commercial exploitation, and grooming tactics used by adults who pose as children or young adults. They will learn how to recognise unsafe interactions, use privacy settings effectively, and report any concerning behaviour or messages to trusted adults and platforms.

Conduct Risks

Pupils will be guided on how their own online behaviour can impact both themselves and others. The curriculum will address the risks associated creating, sharing, or receiving explicit images, including both consensual and non-consensual exchanges of nudes and semi-nudes. Online bullying, including the use of social media and messaging platforms to harass or intimidate others, will also be a key focus. Pupils will be taught responsible digital conduct and the legal and emotional consequences of harmful behaviour.

Commerce Risks

The curriculum will also include education on online commercial risks. Pupils will be informed about the dangers of online gambling, exposure to inappropriate advertising, and financial scams such as phishing. They will learn how to recognise fraudulent schemes, protect their personal and financial information and seek help when confronted with suspicious online activity.

The DSL will be involved with the development of the school's online safety curriculum. Pupils will be consulted on the online safety curriculum, where appropriate, due to their unique knowledge of the kinds of websites they and their peers frequent and the kinds of behaviours in which they engage online.

Relevant members of staff will work together to ensure the curriculum is tailored so that pupils who may be more vulnerable to online harms e.g., receive the information and support they need.

The school will also endeavour to take a more personalised or contextualised approach to teaching about online safety for more susceptible children, and in response to instances of harmful online behaviour from pupils.

Class teachers will review external resources prior to using them for the online safety curriculum, to ensure they are appropriate for the cohort of pupils.

External visitors may be invited into school to help with the delivery of certain aspects of the online safety curriculum. The headteacher and DSL will decide when it is appropriate

to invite external groups into school and ensure the visitors selected are appropriate.

Before conducting a lesson or activity on online safety, the class teacher and DSL will consider the topic that is being covered and the potential that pupils in the class have suffered or may be suffering from online abuse or harm in this way. The DSL will advise the staff member on how to best support any pupil who may be especially impacted by a lesson or activity. Lessons and activities will be planned carefully so they do not draw attention to a pupil who is being or has been abused or harmed online, to avoid publicising the abuse.

During an online safety lesson or activity, the class teacher will ensure a safe environment is maintained in which pupils feel comfortable to say what they feel and ask questions and are not worried about getting into trouble or being judged.

If a staff member is concerned about anything pupils raise during online safety lesson and activities, they will make a report in line with the Safeguarding Policy.

If a pupil makes a disclosure to a member of staff regarding online abuse following a lesson or activity, the staff member will follow the reporting procedure outlined in the Safeguarding Policy.

12. Use of Technology in the Classroom

A wide range of technology will be used during lessons, including the following:

- Computers.
- Laptops.
- Tablets/ iPads/ iPods.
- Internet.
- Email.
- Cameras.
- Other communication devices.
- Other ICT technology such as buttons.

Prior to using any websites, tools, apps or other online platforms in the classroom, or recommending that pupils use these platforms at home, the class teacher will review and evaluate that pupils use these platforms at home, the class teacher will review and evaluate the resource. Class teachers will ensure that any internet-derived materials are used in line with copyright law.

Pupils will be supervised when using online materials during lesson time – this supervision is suitable to their age and ability.

13. Use of Smart Technology

While the school recognises that the use of smart technology can have educational

benefits, there are also a variety of associated risks which this school will ensure it manages.

Pupils will be educated on the acceptable and appropriate use of personal devices and will use technology in line with the school's Acceptable Use Agreement for Pupils.

Staff will use all smart technology and personal technology in line with the school's Acceptable Use Agreement for Pupils and other associated policies (Social Media Policy, Cyber Security Policy, Email Protocol and Retention Policy).

Staff must not use personal mobile devices in classrooms, pupil toilets or changing areas. Mobile phones brought into school are entirely at the staff member, pupil, parent/ carer or visitor's own risk. The school accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school.

The school reserves the right to search the content of any mobile or hand held devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying. Staff mobiles and hand held devices may be searched at any time as part of routine monitoring.

The school recognises that pupils' unlimited and unrestricted access to the internet via mobile phone networks means that some pupils may use the internet in a way which breaches the school's Acceptable Use Agreement for Pupils.

Inappropriate use of smart technology may include:

- Using mobile and smart technology to sexually harass, bully, troll or intimidate peers.
- Sharing indecent images, both consensually and non-consensually.
- Viewing and sharing pornography and other harmful content.

Pupils will not be permitted to use smart devices or any other personal technology whilst in the classroom unless by prior agreement and arrangement with their family.

Pupil mobile phones which are brought into school must be turned off (not placed on silent) and stored out of sight on arrival at school. They must remain turned off and out of sight until the end of the day. Staff members may use their phones during school break times. All visitors are requested to keep their phones on silent.

The school strongly advises that pupil mobile phones should not be brought into school, however this is reviewed on a case-by-case basis. If, as a means to support a child with their regulation on school transport, it is agreed that a pupil can bring their device into school, the class teacher will store the device in a lockable cupboard during the day. The device will be given back to the child at the end of the school day. This will be agreed in advance with the pupil's family.

If a pupil breaches the school's policy, then their phone or device will be confiscated and will be held in a secure place in the school office or classroom. Mobile phones and devices will be released to parents or carers in accordance with school policy.

If a pupil needs to contact their parents/ carers they will be allowed to use a school phone. Families are advised not to contact their child via their mobile phone during the school day, but to contact the school office.

Pupils should protect their phone numbers by only giving them to trusted friends and family members. Pupils will be instructed in safe and appropriate use of mobile phones and personally owned devices and will be made aware of boundaries and consequences.

The school will seek to ensure that it is kept up to date with the latest devices, platforms, apps, trends and related threats.

The school will consider the 4C's (content, contact, conduct and commerce) when educating pupils about the risks involved with the inappropriate use of smart technology and enforcing the appropriate disciplinary measures.

14. Educating Parents

The school will work in partnership with families to ensure pupils stay safe online at school and at home. Parents will be provided with information about the school's approach to online safety and their role in protecting their children. Parents will be sent a copy of the Acceptable Use Agreement at the beginning of each academic year and are encouraged to go through this with their child to ensure their child understands the document and the implications of not following it.

Parents/ Carers will be made aware of the various ways in which their children may be at risk online, including, but not limited to:

- Child sexual abuse, including grooming.
- Exposure to radicalising content.
- Sharing of indecent imagery of pupils e.g., sexting.
- Cyberbullying.
- Exposure to age-appropriate content e.g., pornography.
- Exposure to harmful content e.g., content that encourages self-destructive behaviour.

Parents will be informed of the ways in which they can prevent their child from accessing harmful content at home e.g., by implementing parental controls to block age-inappropriate content.

Parental awareness regarding how they can support their children to be safe online will be raised through a rolling programme of advice, guidance and training for families,

including:

- Information leaflets, in school newsletters, on the school website.
- Suggestions for safe internet use at home.

15. Internet Access

Pupils, staff and other members of the school community will only be granted access to the school's internet network once they have read and signed the Acceptable Use Agreement. A record will be kept of users who have been granted internet access on the school's information management system.

All members of the school community will be encouraged to use the school's internet network, instead of 3G, 4G and 5G networks, as the school network has appropriate filtering and monitoring to ensure individuals are using the internet appropriately.

16. Filtering and Monitoring Online Activity

The governing board will ensure the school's ICT network has appropriate filters and monitoring systems in place and that it is meeting the DfE's ['Filtering and monitoring standards for schools and colleges'](#). The governing board will ensure 'over blocking' does not lead to unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.

The DSL will ensure that specific roles and responsibilities are identified and assigned to manage filtering and monitoring systems and to ensure they meet the school's safeguarding needs.

The headteacher and ICT technicians will undertake a risk assessment to determine what filtering and monitoring systems are required. The filtering and monitoring systems the school implements will be appropriate to pupils' ages, the number of pupils using the network, how often pupils access the network, and the proportionality of costs compared to the risks, ICT technicians will undertake regular checks on the filtering and monitoring systems to ensure they are effective and appropriate.

Requests regarding making changes to the filtering system will be directed to the headteacher. Prior to making any changes to the filtering system, ICT technicians, the DSL and/ or the administration and data manager will conduct a risk assessment. Any changes made to the system will be recorded. Reports of inappropriate websites or materials will be made to an ICT technician immediately, who will investigate the matter under the direction of the administration and data manager, and makes any necessary changes.

Deliberate breaches of the filtering system will be reported to the DSL and administration and data manager, who will escalate the matter appropriately. If a pupil has deliberately breached the filtering system, they will be disciplined in line with the Regulation Support

Policy. If a member of staff has deliberately breached the filtering system, they will be disciplined in line with the Disciplinary Policy and Procedure for Staff.

If material that is believed to be illegal is accessed, inadvertently or deliberately, this material will be reported to the appropriate agency immediately e.g., the Internet Watch Foundation (IWF) CEOP and/ or the Police.

The school's network and school-owned devices will be appropriately monitored. All users of the network and school-owned devices will be informed about how and why they are monitored. Concerns identified through monitoring will be reported to the DSL, who will manage the situation in line with the Safeguarding Policy.

17. Network Security

Technical security features, such as anti-virus software, will be kept up to date and managed by ICT technicians. Firewalls will be switched on at all times. ICT technicians will review the firewalls on a regular basis to ensure they are running correctly, and to carry out any required updates.

Staff and pupils will be advised not to download unapproved software or open unfamiliar email attachments, and will be expected to report all malware and virus attacks to ICT technicians.

All members of staff will have their own unique usernames and private passwords to access the school's systems. Pupils will be provided with their own log in. Staff members and pupils will be responsible for keeping their passwords private. Passwords will have a minimum and maximum length and require a mixture of letters, numbers and symbols to ensure they are as secure as possible.

Users will inform ICT technicians if they target their login details. Users will not be permitted to share their login details with others and will not be allowed to log in as another user at any time. If a user is found to be sharing their login details or otherwise mistreating the password system, the headteacher will be informed and will decide the necessary action to take.

Users will be required to lock access to devices and systems when they are not in use.

The SLT digital lead (DSL) and administration and data manager will be responsible for implementing appropriate network security measures in liaison with the DPO. Full details of the school's network security measures can be found in the Cyber Security Policy.

18. Emails

Access to and use of emails will be managed in line with the Email Protocol and Retention Policy, Data Protection Policy and the Acceptable Use Agreements.

Staff and pupils will be given approved school email accounts and will only be able to use these accounts at school and when doing school-related work outside of school hours. Prior to being authorised to use the email system, staff and pupils must agree to and sign the Acceptable Use Agreement. Personal email accounts will not be permitted to be used on the school site. Any email that contains sensitive or personal information will only be sent using secure and encrypted email.

Staff members and pupils will be required to block spam and junk mail, and report the matter to ICT technicians. The school's monitoring system can detect inappropriate links, malware and profanity within emails – staff and pupils will be made aware of this. Chain letters, spam and all other emails from unknown sources will be deleted without being opened. This will be covered in annual mandatory training modules.

Any cyber attacks initiated through emails will be managed in line with the Cyber Response and Recovery Plan.

19. Generative Artificial Intelligence (AI)

The school will take steps to prepare pupils for changing and emerging technologies e.g., generative AI and how to use them safely and appropriately with consideration given to pupils' age.

The school will ensure its IT system includes appropriate filtering and monitoring systems to limit pupils' ability to access or create harmful or inappropriate content through generative AI.

The school will ensure that pupils are not accessing or creating harmful or inappropriate content including through generative AI.

The school will take steps to ensure that personal and sensitive data is not entered into generative AI tools and that it is not identifiable.

The school will make use of any guidance and support that enables it to have a safe, secure and reliable foundation in place before using more powerful technology such as generative AI.

20. Social Networking

The use of social media by staff and pupils will be managed in line with the school's Social Media Policy.

21. The School Website

The headteacher will be responsible for the overall content of the school website – they will ensure the content is appropriate, accurate, up-to-date and meets government requirements.

The website will be managed by the administration and data manager.

22. Use of Devices

Staff members and pupils will be issued with school-owned devices to assist with their work where necessary. Requirements around the use of school-owned devices can be found in the school's Acceptable Use Agreement.

The use of personal devices on the school premises and for the purposes of school work will be managed in line with the Acceptable Use Agreements and the Safeguarding Pupils Against Mobile Phones, Cameras and Smart Watches Policy.

23. Monitoring and Review

The school recognises that the online world is constantly changing; therefore, the DSL, ICT technicians and the headteacher conduct regular light-touch reviews of this policy to evaluate its effectiveness.

The governing board, headteacher and DSL will review this policy in full on an annual basis and following any online safety incidents.

Any changes made to this policy are communicated to all members of the school community.

Appendix 1 – Acceptable Use Agreement (Staff)

Please sign and return to Tracy De Freitas

Acceptable Use Policy (AUP): Staff agreement form (Dec 2022 version)

Covers use of digital technologies in school or accesses remotely i.e., email, internet and network resources, learning platform, software, equipment and systems.

- I will only use the school's digital technology resources and systems for professional purposes or for uses deemed 'reasonable' by the headteacher and governing board.
- I will not reveal any personal password(s) to anyone.
- I will not allow unauthorised individuals to access email/ internet/ intranet/ network or other school/ LA systems.
- I will ensure all documents, data etc., are saved, accessed and deleted in accordance with the school's network and data security and confidentiality protocols.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will only use the approved, secure email system(s) for any school business which is currently staffmail, unless approved by the headteacher or school business manager.
- I will only use the approved school email, school MLE or other school approved communication systems with pupils or parents/ carers, and only communicate with them on appropriate school business.
- I will not browse, download or send material that could be considered offensive to colleagues.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the appropriate line manager/ e-safety coordinator.
- I will not download any software or resources from the internet that can compromise the network, or are not adequately licenced.
- I will not connect a computer, laptop or other device (including USB flash drive), to the network/ internet that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment updated, using the school's recommended anti-virus, firewall and other ICT 'defence' systems.
- I will not use personal digital cameras or camera phones for taking and transferring images of pupils or staff without permission and will not store images at home without permission.
- If applicable, I will use the school's learning platform in accordance with school/ London Grid for Learning advice.
- I will ensure that any private social media sites/ blogs etc., that I create or actively contribute to are not confused with my professional role, and will not in any way bring the school or colleagues into disrepute by inappropriate postings on social media sites.
- I agree and accept that any computer or laptop loaned to me by the school is provided solely to support my professional responsibilities and that I will notify the school of any "significant personal use" as defined by HM Revenue and Customs.
- I will ensure that any equipment taken out of school on loan other than during school

visits will be my responsibility and should loss/ damage occur, liability will be covered by personal insurances.

- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.
- I understand that the Data Protection Policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, except when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I will embed the school's e-safety curriculum into my teaching.
- I will only use LA systems in accordance with any corporate policies.
- I understand that all internet usage and emails can be logged and this information could be made available to my manager on request.
- I understand that failure to comply with this agreement could lead to disciplinary action.

User Signature

I understand that it is my responsibility to ensure that I remain up to date and read and understand the school's most recent e-safety policies.

I agree to abide by all the points above.

I wish to have an email account, be connected to the intranet and internet and be able to use the school's ICT resources and systems.

Signature..... Date.....

Full Name..... (printed)

Job Title.....

School.....

Authorised Signature – Administration and Data Manager

I approve this user to be set-up

Signature..... Date.....

Full Name..... (printed)

Appendix 2 – Acceptable Use Agreement (Pupils)

Online Safety Form for Pupils

Think before you click



I will only use the Internet and email with an adult



I will only click on icons and links when I know they are safe



I will only send friendly and polite messages



If I see something I don't like on a screen, I will always tell an adult

My Name:

My Signature:

12 Rules for Responsible ICT Use

These rules will keep everyone safe and help us to be fair to others.

- I will only use the computers for schoolwork and homework.
- I will only delete my own files.
- I will not look at other people's files without their permission.
- I will keep my login and password secret.
- I will not bring files into school without permission.
- I will ask permission from a member of staff before using the Internet and will not visit Internet sites I know to be banned by the school.
- I will only e-mail people I know, or my teacher has approved.
- The messages I send, or information I upload, will always be polite and sensible.
- I will not open an attachment, or download a file, unless I have permission or I know and trust the person who has sent it.
- I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless my teacher has given permission.
- I will never arrange to meet someone I have only ever previously met on the Internet or by email or in a chat room, unless my parent, guardian or teacher has given me permission and I take a responsible adult with me.
- If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will tell a teacher / responsible adult.

Appendix 3 – Acceptable Use Agreement Including Photo/ Video Permission (Parents/ Carers)

Parent/ Guardian Name.....

Pupil Name(s).....

As the parent or legal guardian of the above pupil(s), I grant permission for my child to have access to use the internet, London Grid for Learning (LGfL) email and other ICT facilities at school.

I know that where appropriate my child has signed an e-safety agreement form and has been shown the '12 rules for responsible ICT use'.

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the internet and mobile technologies, but I understand that the school will take every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. These steps include using an educationally filtered service, restricted access email, employing appropriate teaching practice and teaching e-safety skills to pupils.

I understand that the school can check my child's computer files, and the internet sites they visit, and that if they have concerns about their e-safety or e-behaviour that they will contact me.

I will support the school by promoting safe use of the internet and digital technology at home and will inform the school if I have any concerns over my child's e-safety.

Parent/ guardian signature.....

Date.....

Use of digital Images – Photography and Video: I also agree to the school using photographs of my child or including them in video material, as described in the document 'Use of digital and video images'. I have read and understood this document. I understand that images will only be used to support learning activities or in publicity that reasonably promotes the work of the school, and for no other purpose.

Parent/ guardian signature.....

Date.....

Use of digital images – photography and video

To comply with the Data Protection Act 1998, we need your permission before we can photograph or make recordings of your daughter/ son.

We observe the following rules for an external use of digital images:

- If the pupil is named, we avoid using their photograph.
- If their photograph is used, we avoid naming the pupil.

Where showcasing examples of pupil's work we only use their first names, rather than their full names.

If showcasing digital work to an external audience, we take care to ensure that pupils aren't referred to by name on the video, and that pupils' full names aren't given in credits at the end of the film.

Only images of pupils in suitable dress are used.

Staff are not allowed to take photographs or videos on their personal equipment.

Examples of how digital photography and video may be used include:

- Your child being photographed (by the classroom teacher, teaching assistant or another child) as part of a learning activity e.g., photographing children at work and then sharing the pictures on the interactive whiteboard in the classroom allowing the children to see their work and make improvements.
- Your child's image for presentation purposes around the school e.g., in school wall displays and PowerPoint presentations to capture images around the school or in the local area as part of a project or lesson.
- Your child's image being used in a presentation about the school and its work in order to share its good practice and celebrate its achievements, which is shown to other parents, schools or educators e.g., within a CDROM/ DVD or a document sharing good practice, in our school prospectus or on our school website.
- In rare events, your child could appear in the media if a newspaper photographer or television crew attend an event.

Note: If we, or you, actually wanted your child's image linked to their name we would contact you separately for permission e.g., if your child won a national competition and wanted to be named in local or government literature.

Appendix 4 – Protocol for Responding to Online Safety Infringements

Whenever a pupil or staff member infringes the E-Safety Policy, the final decision on the level of sanction will be at the discretion of the school management and will reflect the school's behaviour and disciplinary procedures.

The following are provided as exemplification only:

PUPIL	
Category A Infringements	Possible Sanctions
• Use of non-educational sites during lessons • Unauthorised use of email • Unauthorised use of mobile phone (or other new technologies) in lessons e.g., to send texts to friends • Use of unauthorised instant messaging/ social networking sites	Refer to class teacher Escalate to: senior manager/ e-safety coordinator
Category B Infringements	Possible Sanctions
• Continued use of non-educational sites during lessons after being warned • Continued unauthorised use of email after being warned • Continued unauthorised use of mobile phone (or other new technologies) after being warned • Continued use of unauthorised instant messaging/ chatrooms, social networking sites, NewsGroups • Use of filesharing software e.g., Napster, Vanbasco, BitTorrent, LiveWire etc. • Trying to buy items online • Accidentally corrupting or destroying others' data without notifying a member of staff of it • Accidentally accessing offensive material and not logging off or notifying a member of staff of it	Refer to class teacher/ senior manager/ e-safety coordinator Escalate to: removal of internet access rights for a period, removal of phone until end of school day, contact with parent/ guardian
Category C Infringements	Possible Sanctions
• Deliberately corrupting or destroying someone's data, violating privacy of others or posts inappropriate messages, videos or images on a social networking site • Sending an email or MSN message that is regarded as harassment or of a bullying nature (one-off) • Purchasing or ordering of items online • Transmission of commercial or advertising material	Refer to class teacher/ senior manager/ e-safety coordinator/ headteacher/ removal of internet access rights for a period. Escalate to: contact with parent/ guardian, removal of equipment Other possible safeguarding actions if inappropriate web material is accessed: Ensure appropriate technical support filters the site
Category D Infringements	Possible Sanctions
• Continued sending of emails or MSN messages regarded as harassment or of a bullying nature after being warned • Deliberately creating, accessing, downloading or disseminating any material deemed	Refer to headteacher/ contact with parents Other possible safeguarding actions: • Secure and preserve any evidence

offensive, obscene, defamatory, racist, homophobic or violent • Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act 1998 • Bringing the school's name into disrepute	• Inform the sender's email service provider • Liaise with relevant service providers/ instigators of the offending material to remove • Report to Police/ CEOP where child abuse or illegal activity is suspected.
---	---

STAFF	
Category A Infringements (Misconduct)	Possible Sanctions
• Excessive use of internet for personal activities not related to professional development e.g., online shopping, personal email, instant messaging etc. • Use of personal data storage media e.g., USB memory sticks) without considering access and appropriateness of any files stored • Not implementing appropriate safeguarding procedures • Any behaviour on the worldwide web that compromises the staff members' professional standing in the school and community • Misuse of first level data security e.g., wrongful use of passwords • Breaching copyright or licence e.g., installing unlicensed software on network	Referred to line manager/ headteacher Escalate to: warning given
Category B Infringements (Gross Misconduct)	Possible Sanctions
• Serious misuse of, or deliberate damage to, any school/ council computer hardware or software • Any deliberate attempt to breach data protection or computer security rules • Deliberately creating, accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent • Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act 1998 • Bringing the school name into disrepute	Referred to headteacher/ governors Escalate to: report to LA/ LSCB, Personnel and HR. Report to Police/ CEOP where child abuse or illegal activity is suspected. Other possible safeguarding actions: • Remove the PC/ laptop to a secure place to ensure there is no further access • Instigate an audit of all ICT equipment by an outside agency to ensure no risk of pupils accessing inappropriate materials in the school • Identify the precise details of the material

If a member of staff commits an exceptionally serious act of gross misconduct:

The member of staff should be instantly suspended. Normally though, there will be an investigation before disciplinary action is taken for any alleged offence. As part of that the member of staff will be asked to explain their actions and these will be considered before any disciplinary action is taken.

Schools are likely to involve external support agencies as part of these investigations e.g., an ICT technical support service to investigate equipment and data evidence, the local authority HR team etc.

Child abuse images found:

In the case of child abuse images being found, the member of staff should be immediately suspended and the Police should be called.

Anyone may report any inappropriate or potentially illegal activity or abuse with or towards a child online to the Child Exploitation and Online Protection (CEOP):

<https://www.ceop.police.uk/Safety-Centre/>

<https://www.iwf.org.uk/>

How will staff and pupils be informed of these procedures?

- They will be fully explained and included in the school's E-Safety Policy and acceptable use agreements. All staff will be required to sign the school's e-safety acceptable use agreement form.
- Pupils will be taught about responsible and acceptable use and given strategies to deal with incidents so they can develop 'safe behaviours'. Pupils will sign an age-appropriate e-safety/ acceptable use agreement form.
- The school's e-safety policy will be made available and explained to parents, and parents will sign an acceptance form when their child starts at the school.
- Information on reporting abuse/ bullying etc. will be made available by the school for pupils, staff and parents.
- Staff are issued with the 'What to do if?' guide on e-safety issues (see LGfL safety site).