Acceptable Use of Information Technology, Online Safety and Cyber-Abuse Policy

November 2026

Date of next review November 2027

Approved by:	**The Governing Board**	**Date:**
Version Number:	2.0	13/07/2026
Last reviewed on:	[To be completed]	
Next review due by:	[To be completed]	

Contents

1. Policy Overview and Scope
2. Our Commitment to Equality and Inclusion
3. Acceptable Use of ICT
4. Digital Accessibility and Reasonable Adjustments
5. Unacceptable Behaviour
6. Procedures for ICT Use
7. Electronic Mail (E-Mail)
8. Passwords and Security
9. USB Storage
10. Pupil ICT Use
11. Staff ICT Use
12. Mobile Phones
13. Photography and Images
14. Cyber-Bullying
15. Identity-Based Cyber-Bullying
16. E-Safety
17. Recognition and Response to Online Abuse
18. Reporting Procedures
19. Education
20. Infringements and Sanctions
21. Rewards

22. Monitoring and Review

23. Agreement

---

1. Policy Overview and Scope

This policy applies to all staff including those that are part-time, visitors, agency staff, contractors and to those using the school's ICT resources. For the purposes of this document the 'internet' is defined as; web services, chat rooms, internet mail, bulletin boards, newsgroups, peer to peer file sharing and instant messaging software including smart watches.

This policy aims to ensure that all communications technology (including computers, mobile devices and mobile phones) is used to support learning without creating unnecessary risk to users, whilst actively promoting equality and protecting all members of our school community from online harm.

Accessibility of this Policy

This policy is available in alternative formats upon request, including:

- Large print
- Audio format
- Easy-read version
- Translated versions
- Screen-reader compatible digital format

Please contact the e-Safety Coordinator if you require this policy in an alternative format.

---

2. Our Commitment to Equality and Inclusion

2.1 Equality Statement

This policy has been developed with due regard to the Public Sector Equality Duty under the Equality Act 2010. The school is committed to eliminating discrimination, harassment, and victimisation in online contexts; advancing equality of opportunity in access to ICT and online safety; and fostering good relations through inclusive online practices and education that challenges discrimination.

We are committed to ensuring that:

- All students and staff can access and use ICT systems safely and effectively, regardless of protected characteristics

- Online safety education addresses the diverse needs and specific risks faced by all members of our school community
- Identity-based cyber-bullying and online discrimination are recognised as serious safeguarding concerns
- ICT systems, resources, and online safety support are accessible to everyone
- Monitoring, reporting, and sanctioning procedures are applied fairly and without discrimination

2.2 Recognizing Diverse Online Safety Needs

The school recognizes that students hold multiple identities and may face compounded online safety risks due to intersecting protected characteristics. For example, LGBTQ+ students from minority ethnic backgrounds may face both racist and homophobic cyber-bullying. Online safety support will address students' whole identities and intersecting vulnerabilities.

We acknowledge that certain groups face disproportionate online risks:

LGBTQ+ Students: The school recognizes that LGBTQ+ students face significantly elevated risks of online abuse including homophobic, biphobia, and transphobic cyber-bullying, online outing, and targeted harassment. All such incidents will be treated as serious safeguarding concerns.

Transgender Students: The school recognizes that transgender students face significantly elevated risks of online abuse including transphobic cyber-bullying, online outing, misgendering, deadnaming, and sharing of pre-transition images. All such incidents will be treated as serious safeguarding concerns.

Students from Minority Ethnic Backgrounds: The school recognizes that students from minority ethnic backgrounds may face racist cyber-bullying, online hate speech, and racial harassment. All racist online content, comments, and behaviour will be treated as serious safeguarding concerns and will be addressed through the school's anti-bullying and safeguarding procedures.

Disabled Students: The school recognizes that disabled students may be more vulnerable to online grooming, cyber-bullying, and exploitation. Staff will be particularly vigilant in monitoring online safety for disabled students and will provide tailored e-safety education that addresses their specific vulnerabilities. Disability-based cyber-bullying (ableist language, mocking, harassment related to disability) will be treated as a serious safeguarding concern and will be addressed through the school's anti-bullying and safeguarding procedures.

Female Students: The school recognizes that girls face specific online risks including online sexual harassment, image-based sexual abuse (sharing of intimate images without consent), online grooming for sexual exploitation, gender-based cyber-bullying (slut-shaming, appearance-based bullying), and pressure to share sexual images. All such incidents will be treated as serious safeguarding concerns. The school recognizes that students who have experienced previous exploitation, trafficking, or abuse may be particularly vulnerable to online sexual exploitation and will provide tailored e-safety education and monitoring.

Students from Religious Backgrounds: The school recognizes that students from certain religious backgrounds may face religiously motivated cyber-bullying including Islamophobic, anti-Semitic, or other religious harassment. All religiously motivated online abuse will be treated as serious safeguarding concerns.

Pregnant Students and Young Mothers: Cyber-bullying related to pregnancy or maternity (shaming, judgmental comments, sharing of pregnancy-related images without consent, privacy violations) will be treated as a serious form of cyber-bullying and addressed through safeguarding procedures.

---

3. Acceptable Use of ICT

Use of the internet by employees of Physis is permitted and encouraged where such use supports the goals and objectives of the business, sharing and storing of secure information, preparing resources and relevant documentation required and to enable efficient communication between Physis staff and outside agencies.

However, employees must ensure that they:

- Comply with current legislation, including the Equality Act 2010
- Use the internet in an acceptable way that respects the dignity and rights of all users
- Understand that use of the internet is monitored for security and network management reasons
- Recognize that the distribution of any information through the school's network is subject to scrutiny
- Understand that the use of computing resources is subject to UK law and any illegal use will be dealt with appropriately
- Do not use the internet and social media in a way that may compromise the reputation of Physis, including through discriminatory, harassing, or offensive content

- Do not share the location of the school
- Do not leave school devices where they can be accessed by anybody other than the intended user, including when devices are taken offsite
- Do not access the internet using a public Wi-Fi connection

Physis accepts that the use of the internet is an extremely valuable business, research and learning tool. However, misuse of such facility can have a detrimental effect on other users and potentially the organisations public profile. As a result, the organisation monitors the use of the internet via InfoSol via WatchGuard technology.

Fair and Non-Discriminatory Monitoring

Internet monitoring will be applied fairly and without discrimination. The school will monitor whether certain groups of students are disproportionately flagged for online behaviour and will address any bias in monitoring practices.

The school monitors:

- The volume of internet and network traffic
- The internet sites visited, by whom and time and date

The specific content of any transactions will not be monitored unless there is a suspicion of improper use.

We are obliged to monitor to fulfil our responsibilities regarding UK law. Actions deemed appropriate by the Head of Service may be taken.

---

4. Digital Accessibility and Reasonable Adjustments

4.1 Legal Duty

The school has a legal duty under the Equality Act 2010 to make reasonable adjustments for disabled students. All ICT systems, equipment, and online resources will be accessible to disabled students.

4.2 Accessible ICT Systems

We are committed to ensuring that all ICT systems are accessible to disabled students. This includes:

For students with visual impairments:

- Screen readers
- Large text options

- High contrast displays
- Alternative text for images
- Magnification software

For students with hearing impairments:

- Captions for videos
- Visual alerts instead of audio notifications
- Transcripts for audio content

For students with motor difficulties:

- Alternative input devices (voice control, adapted keyboards/mice, eye-gaze technology)
- Adjustable response times
- Keyboard shortcuts
- Touch screen options

For students with learning disabilities:

- Simplified interfaces
- Clear navigation
- Accessible language
- Text-to-speech functionality
- Spell-checkers and grammar support
- Visual supports and concrete examples

For autistic students:

- Predictable layouts
- Reduced sensory elements (option to disable flashing, sounds)
- Clear instructions
- Structured interfaces

For students with dyslexia:

- Text-to-speech
- Dyslexia-friendly fonts
- Spell-checkers

- Adjustable text spacing and formatting

4.3 Requesting Reasonable Adjustments

Students who require reasonable adjustments to access ICT systems should discuss their needs with their teacher, the SENDCo, or the e-Safety Coordinator at the earliest opportunity. All discussions will be treated confidentially, and adjustments will be reviewed regularly to ensure they remain appropriate.

Reasonable adjustments may also include:

- Extended time for online activities
- Alternative methods for completing online tasks
- Flexible deadlines
- Additional support from staff
- Adapted assessment methods

4.4 Accessible E-Safety Education

E-safety education will be accessible to all students, including students with learning disabilities (simplified language, visual supports, concrete examples), students with sensory impairments (captions, visual/audio alternatives), and students with communication difficulties (alternative reporting methods).

4.5 Important Note on Disability and Sanctions

Disability or health conditions will never be confused with underperformance or breach of this policy. When applying sanctions, staff will consider whether online behaviour is related to disability (e.g., autistic students may struggle with social communication online), communication difficulties, or cultural differences in online communication. Reasonable adjustments will be made where appropriate.

---

5. Unacceptable Behaviour

The following is deemed unacceptable use or behaviour by employees and students:

- Visiting internet sites that contain obscene, hateful, pornographic or otherwise illegal material
- Using the computer to perpetrate any form of fraud or software, film or music piracy

- Using the internet to send offensive or harassing material to other users
- Visiting internet sites, making, posting, downloading, uploading or passing on material, remarks, proposals or comments that contain or relate to:
    - Inappropriate images
    - Promoting discrimination of any kind, including racist, homophobic, biphobic, transphobic, ableist, Islamophobic, anti-Semitic, or sexist content
    - Promoting violence or bullying
    - Promoting racial or religious hatred
    - Promoting illegal acts
    - Breaching any Local Authority/School policies
- Downloading commercial software or any copyrighted materials belonging to third parties, unless this download is covered or permitted under a commercial agreement or other such licence
- Hacking into unauthorised areas
- Publishing defamatory and/or knowingly false material about Physis, colleagues, students, or community members on social networking sites, 'blogs', 'wikis' and any online publishing format
- Revealing confidential information about Physis or personal information about students, staff, or community members
- Undertaking deliberate activities that waste staff effort or networked resources
- Intentionally interfering with the normal operation of the network, including the propagation of computer viruses
- Referring or referencing any of Physis' homes, schools, residents, staff or others on social networking sites

Identity-Based Discrimination Online

All forms of identity-based discrimination, harassment, and abuse online are strictly prohibited and will be treated as serious safeguarding concerns. This includes but is not limited to:

- **Racist content, comments, or behaviour** - racial slurs, racist "jokes", sharing of racist images/memes, racial microaggressions

- **Homophobic, biphobic, and transphobic content, comments, or behaviour** - LGBTQ+-related slurs, harassment, "jokes", misgendering, deadnaming
- **Ableist content, comments, or behaviour** - disability-related slurs, mocking, harassment related to disability
- Islamophobic, anti-Semitic, or other religiously motivated content, comments, or behaviour
- **Sexist content, comments, or behaviour** - gender-based harassment, slut-shaming, appearance-based bullying, online sexual harassment
- **Pregnancy-related harassment** - shaming, judgmental comments, privacy violations

---

6. Procedures for ICT Use

Electronic media may not be used for knowingly transmitting, retrieving or storage of any communications of a discriminatory or harassing nature, or which are derogatory to any individual or group, or which are obscene or X-rated communications, or are of a defamatory or threatening nature, or for "chain letters," or for any other purpose which is illegal or against company policy or contrary to the company's interest.

This includes all forms of identity-based discrimination and harassment as outlined in Section 5.

- Electronic media and services are primarily for school business use. Employees are not permitted to use the school's electronic services for personal use
- The school reserves the right, in its discretion, to review any employee's electronic files and messages and usage to the extent necessary to ensure that electronic media and services are being used in compliance with the law and with this and other school policies
- Employees should therefore not assume electronic communications are totally private and confidential and should transmit highly sensitive personal information in other ways
- Employees must respect the confidentiality of other people's electronic communications and may not attempt to read, "hack" into other systems or other people's logins, or "crack" passwords, or breach computer or network security measures, or monitor electronic files or communications of other employees or third parties except by explicit direction of Senior Leadership Team

- No e-mail or other electronic communications may be sent which attempt to hide the identity of the sender or represent the sender as someone else or from another organization
- Electronic media and services should not be used in a manner that is likely to cause network congestion or significantly hamper the ability of other people to access and use the system
- Anyone obtaining electronic access to other companies' or individuals' materials must respect all copyrights and may not copy, retrieve, modify or forward copyrighted materials except as permitted by the copyright owner or a single copy for reference use only
- Staff should be aware that network services and World Wide Web sites can and do monitor access and usage and can identify at least which organization -- and often which specific individual -- is accessing their services
- Any employee found to be abusing the privilege of school-facilitated access to electronic media or services will be subject to disciplinary corrective action and/or risk having the privilege removed

---

7. Electronic Mail (E-Mail)

Physis provides an email system to support its activities and research and to assist in communication for Physis staff and teams. Emails sent or received on the school email system are not private property; they form part of the administrative records of the school.

Incidental and occasional personal use of the corporate email system is permitted, subject to the restrictions contained in this policy. Any personal use of email is expected to be on the employee's own time and is not to interfere with the person's job responsibilities. Personal use of the email system must not be detrimentally affecting the job responsibilities of other employees, disrupt the system and/or harm the school's reputation.

Care should be taken when using email because messages are perceived to be less formal than paper-based communication and there is a tendency to be lax about their content. Bear in mind that all expressions of fact, intention and opinion via email can be held against you and/or the school in the same way as verbal and written expressions.

Emails must not contain any discriminatory, harassing, or offensive content as outlined in Section 5.

All information relating to our students and the business operation of the school is confidential. You are expected to treat electronic information with the same care as you would paper-based information which is confidential.

Keep all such information secure, use it only for the purpose(s) intended and do not disclose the same to any unauthorised third party.

Exercise due care when writing an email to avoid being rude or unnecessarily terse and ensure that your message meets the standards of professionalism the school expects of your position. Do not make any statements on your own behalf or on behalf of the school, which do or may defame, libel or damage the reputation of any person.

Email messages that have been deleted from the system can be traced and retrieved. Therefore, all persons having a part in creating or forwarding any offending email can be identified. Emails, both in hard copy and in electronic form, are admissible in a Court of law.

All ICT equipment is property of Physis and personal equipment is not to be used. All connections set up by InfoSol must not be changed as this may alter the security of the network.

---

8. Passwords and Security

Ensure that personal passwords are not easy to figure out and are kept private. A log of pupil usernames and passwords can be collected via a spreadsheet on the SharePoint. These details are to be added by education staff using the spreadsheet provided and saved in white text to prevent usernames and passwords from being seen.

You must not access another person's computer or user account. Staff can assist with ICT issues, sharing good practice and upskilling but they are only able to access user accounts and equipment with permission. However, they must not have access to their username and password.

Correct Names and Identifiers in ICT Systems

ICT systems will use students' correct names, pronouns, and gender markers. Students who transition will be able to change usernames, email addresses, and other identifiers to reflect their correct identity. Confidentiality about students' transgender status will be maintained in all online systems.

Students who need to change their name, username, or other identifiers in ICT systems should speak to the e-Safety Coordinator or a trusted member of staff. All such requests will be handled confidentially and sensitively.

Software Updates, Firewalls, and Anti-Virus Software

All the school's ICT devices that support software updates, security updates, and anti-virus products will be configured to perform such updates regularly or automatically.

Users must not circumvent or make any attempt to circumvent the administrative, physical and technical safeguards we implement and maintain to protect personal data and the school's ICT facilities.

Data Protection

All personal data must be processed and stored in line with data protection regulations and the school's data protection policy.

Particular care must be taken with personal data relating to protected characteristics, including information about students' or staff members' disability, gender identity, sexual orientation, religious beliefs, ethnicity, or pregnancy. This information will only be shared on a need-to-know basis and with explicit consent, except where disclosure is required by law or necessary for safeguarding.

Access to Facilities and Materials

All users of the school's ICT facilities will have clearly defined access rights to school systems, files and devices.

Users should not access, or attempt to access, systems, files or devices to which they have not been granted access. If access is provided in error, or if something a user should not have access to is shared with them, they should alert David Lyon immediately.

Users should always log out of systems and lock their equipment when they are not in use to avoid any unauthorised access. Equipment and systems should always be logged out of and closed completely at the end of each working day.

---

9. USB Storage

Whilst USB sticks provide a risk to the integrity of the network, it is appreciated that with the limited computer connectivity and the use of multiple classrooms, office space and workstations USB storage is required. However, they can easily introduce viruses etc to the network. To minimise the risk to the network the following must be adhered to:

- No Personal USB sticks are to be used on any school computer equipment
- Do not use the sticks on any untrusted computer device i.e. your friend's laptop. Ensure that any device you connect them to does have up to date anti-virus software
- Do not let anyone else use the sticks, only you are allowed to transfer files on and off the stick

- Only documents relating to your role in the school are to be stored on these devices
- Do not store confidential or sensitive information on these devices as they are small and easily be misplaced or go missing

---

10. Pupil ICT Use

Pupils are to be introduced to the ICT Code of Conduct and must read and sign in agreement with these conditions to fully understand what is expected of them. Failure to agree with the Code of Conduct and a breach in adhering to it will require intervention as to how and why this has occurred. This must be logged in pupil folders and work completed to determine the level of understanding in that area.

When working with pupils who have breached the ICT Code of Conduct, staff will consider:

- Whether the breach is related to disability (e.g., difficulty understanding social norms online, communication difficulties)
- Whether the pupil requires additional support or reasonable adjustments
- Whether the breach is related to lack of understanding rather than deliberate misconduct
- The pupil's individual circumstances and vulnerabilities

Once there is sufficient reason to move forward the pupil may feel they are ready to sign/agree to the Code of Conduct and can therefore have a username and password set up on each computer.

Pupils are not permitted to use mobile phones, USB devices of any kind, media streaming services and social media whilst at school. ICT and internet use is for the sole purpose of education.

Under the Education Act 2011, and in line with the Department for Education's guidance on searching, screening and confiscation, the school has the right to search pupils' computers for any harmful or inappropriate content that is in breach of the ICT Code of Conduct.

The school can, and will, delete files and data found on searched devices if we believe the data or file has been, or could be, used to disrupt teaching or break the school's rules.

Age-Appropriate Online Safety

E-safety education and monitoring will be age-appropriate and developmentally sensitive, recognizing that online risks and behaviours vary by age and stage.

We recognize that students aged 11-18 have different online safety needs:

- Younger students (11-13) may need more scaffolded e-safety education and closer monitoring
- Older students (14-16) face increased peer pressure and may engage in riskier online behaviour
- Students approaching 18 need preparation for independent online safety and digital citizenship

---

11. Staff ICT Use

Staff must not add pupils as friends in social networking sites. Staff must not post pictures of school events Staff must not use social networking sites within lesson times Staff need to use social networking in a way that does not conflict with the GTC code of conduct, TDA Core Standards or Personnel handbook Staff should review and adjust their privacy settings to give them the appropriate level of privacy

Staff as Role Models for Inclusive Online Conduct

All staff will receive training on equality, diversity, and online safety, including recognizing and responding to identity-based cyber-bullying (racist, homophobic, transphobic, ableist, Islamophobic, sexist); supporting LGBTQ+ students online; cultural competence in online contexts; and addressing unconscious bias in monitoring and sanctioning online behaviour.

Staff should:

- Model inclusive, respectful online conduct
- Challenge discrimination, harassment, and hate speech online (in professional contexts)
- Support students experiencing identity-based cyber-bullying
- Be aware of unconscious bias in monitoring and sanctioning online behaviour
- Understand the specific online safety risks faced by students with protected characteristics

Important: Being open about one's identity (including sexual orientation, gender identity, religious beliefs, etc.) on social media is not unprofessional.

"Professional presence" means respectful and appropriate conduct, not hiding one's identity.

---

12. Mobile Phones

Staff personal mobile phones are not to be used during lesson times, placed on silent and are to be stored away from the classrooms. Staff are not to use their personal phones in front of students at any time. On trips the school mobile phone needs to be taken for communication. Pupils are not allowed mobile phones in school or education trips.

---

13. Photography and Images

Only the school cameras must be used to take photographs for pupils for educational purposes and only to be used within school. Permission must be sought from parent/legal guardian. These must be appropriate and secure; they are not to be used on social media and posted on websites. Pupils who are uncomfortable with having their picture taken may choose not to have their photo taken. If photographs are required for course work evidence, this needs to conform with the requirements of the course. Photos taken by School are subject to the Data Protection Act.

Protection from Image-Based Abuse

Sharing of intimate or sexual images without consent (including 'revenge porn', sexual extortion, peer pressure to share images) will be treated as a serious safeguarding concern and will be reported to police and CEOP where appropriate.

The following are strictly prohibited and will be treated as serious safeguarding concerns:

- Sharing of intimate images without consent
- Sharing of pre-transition images of transgender students without consent
- Sharing of pregnancy-related images without consent
- Using images to shame, harass, or bully students
- Coercing or pressuring students to share images

---

14. Cyber-Bullying

"Cyber-bullying is an aggressive, intentional act carried out by a group or individual, using electronic forms of contact, repeatedly over time against a victim who cannot easily defend him or herself."

We recognise that the advent of cyber-bullying adds a new and worrying dimension to the problem of bullying as there is no safe haven for the person being bullied. Unlike other forms of bullying, cyber-bullying can follow children and young people into their private spaces and outside school hours. Cyber-bullies can communicate their messages to a wide audience with remarkable speed and can often remain unidentifiable and unseen.

Eight Categories of Cyber-Bullying

We have identified eight categories of cyber-bullying:

1. **Text message bullying** - involves sending unwelcome texts that are threatening or cause discomfort
2. **Picture/video-clip bullying via mobile phone cameras** - is used to make the person being bullied feel threatened or embarrassed, with images usually sent to other people. 'Happy slapping' involves filming and sharing physical attacks
3. **Phone call bullying via mobile phone** - uses silent calls or abusive messages. Sometimes the bullied person's phone is stolen and used to harass others, who then think the phone owner is responsible
4. **Email bullying** - uses email to send bullying or threatening messages, often using a pseudonym for anonymity or using someone else's name to pin the blame on them
5. **Online grooming, Chat room and Social Networking Site abuse** - involves sending menacing or upsetting responses to children or young people
6. **Bullying through instant messaging (IM)** - is an Internet-based form of bullying where children and young people are sent unpleasant messages as they conduct real-time conversations online
7. **Bullying via websites** - includes the use of defamatory blogs (web logs), personal websites and online personal polling sites
8. **Identity-based cyber-bullying** - See Section 15 below

Because of the anonymity that new communications technologies offer, anyone with a mobile phone or Internet connection can be a target for cyber-bullying. Furthermore, bullies can reach much larger numbers within a peer group than they can with conventional bullying. Although it leaves no visible scars, cyber-bullying of all types can be extremely destructive.

We will offer parents' information sessions on the dangers of cyber-bullying and on-line child protection issues at regular intervals, including information on identity-based cyber-bullying and how to support children from diverse backgrounds.

---

15. Identity-Based Cyber-Bullying

Identity-based cyber-bullying involves targeting individuals based on protected characteristics including race, religion, disability, sexual orientation, gender identity, sex, or pregnancy. This includes racist, Islamophobic, anti-Semitic, homophobic, biphobic, transphobic, ableist, and sexist cyber-bullying. Identity-based cyber-bullying is a serious safeguarding concern and hate incident.

Recognizing Disproportionate Targeting

The school recognizes that students with certain protected characteristics (LGBTQ+ students, disabled students, students from minority ethnic backgrounds, students from certain religious backgrounds) face disproportionate rates of cyber-bullying and will provide tailored support and monitoring.

Specific Forms of Identity-Based Cyber-Bullying

Racist Cyber-Bullying: Staff will be trained to recognize and respond to racist cyber-bullying, including racial slurs, racist 'jokes', sharing of racist images/memes, and racial microaggressions online.

This includes:

- Racial slurs and offensive language
- Racist "jokes" or memes
- Sharing of racist images or videos
- Racial microaggressions
- Cultural appropriation and mocking
- Targeting based on ethnicity, nationality, or skin colour

Homophobic, Biphobic, and Transphobic Cyber-Bullying: Homophobic, biphobic, and transphobic online content, comments, and behaviour will be addressed through the school's anti-bullying and safeguarding procedures.

This includes:

- LGBTQ+-related slurs and offensive language

- Homophobic, biphobic, or transphobic "jokes"
- Misgendering or deadnaming transgender students
- Mocking or harassment related to sexual orientation or gender identity
- Sharing of pre-transition images without consent
- Targeted harassment campaigns

Online Outing: Online outing (revealing a student's sexual orientation or gender identity without consent) will be treated as a serious form of cyber-bullying and potential safeguarding concern.

Online outing is when someone reveals another person's sexual orientation or gender identity without their consent. This is a serious breach of privacy and can put students at risk of harm. Any incidents of online outing will be treated as urgent safeguarding concerns.

Ableist Cyber-Bullying: Disability-based cyber-bullying includes:

- Ableist slurs and offensive language
- Mocking or harassment related to disability
- Sharing of images or videos that mock disabled people
- Excluding disabled students from online activities
- Making fun of accessibility needs or assistive technology

Islamophobic, Anti-Semitic, and Other Religiously Motivated Cyber-Bullying: Filtering systems will block content promoting religious hatred. Staff will be trained to recognize and respond to religiously motivated cyber-bullying.

This includes:

- Religious slurs and offensive language
- Mocking of religious practices (e.g., wearing hijab, religious observance)
- Sharing of religiously offensive images or content
- Targeting based on religious beliefs or practices
- Hate speech targeting religious groups

Sexist and Gender-Based Cyber-Bullying: This includes:

- Sexist slurs and offensive language

- Slut-shaming and appearance-based bullying
- Online sexual harassment (unwanted sexual comments, requests for nude images)
- Sharing of intimate images without consent
- Pressure to share sexual images
- Gender-based harassment and misogyny

Pregnancy-Related Cyber-Bullying: This includes:

- Shaming or judgmental comments about pregnancy
- Sharing of pregnancy-related images without consent
- Privacy violations regarding pregnancy information
- Harassment or exclusion related to pregnancy or maternity

Responding to Identity-Based Cyber-Bullying

All incidents of identity based cyber-bullying will be treated as serious safeguarding concerns and will be addressed through the school's anti-bullying and safeguarding procedures.

Staff will receive specific training on:

- Recognizing different forms of identity-based cyber-bullying
- Understanding the specific vulnerabilities of students with protected characteristics
- Responding sensitively and effectively to reports of identity-based abuse
- Supporting victims and addressing perpetrators appropriately
- Reporting hate incidents to appropriate authorities

---

16. E-Safety

The Child Exploitation and Online Protection Centre (CEOP) brings together law enforcement officers, specialists from children's charities and industry to tackle online child sexual abuse. CEOP provides a dedicated 24-hour online facility for reporting instances of online child sexual abuse.

Filtering and Monitoring Systems

Filtering systems will block harmful content including racist, homophobic, biphobic, transphobic, ableist, Islamophobic, and other hate speech content,

as well as extremist and radicalizing content. However, filtering will not block legitimate LGBTQ+ support resources, mental health support, or other affirming content that students may need to access.

Students who find that legitimate educational or support resources have been blocked can request access through the e-Safety Coordinator. All such requests will be handled confidentially and sensitively.

Online Radicalization

The school recognizes that vulnerable students may be targeted for radicalization online. E-safety education will include teaching about online radicalization, extremist content, and how to report concerns. Staff will be trained to recognize signs of online radicalization.

---

17. Recognition and Response to Online Abuse

The impact on a child of ICT-based sexual abuse is similar to that for all sexually abused children, however, it has an additional dimension, as there is a visual record of the abuse. ICT-based sexual abuse of a child constitutes significant harm through sexual and emotional abuse.

All adults (volunteers, staff) working with children, adults and families will be alerted to the possibility that:

- A child may already have been/is being abused and the images distributed on the internet or by mobile telephone
- An adult or older child may be grooming a child for sexual abuse, including for involvement in making abusive images
- An adult or older child may be viewing and downloading child sexual abuse images

Online Sexual Harassment and Image-Based Sexual Abuse

Students will be taught about the risks of sharing intimate images, the law around image-based sexual abuse, and how to report concerns.

Online sexual harassment (unwanted sexual comments, requests for nude images, sexual cyber-bullying) will be treated as a form of sexual harassment under the school's safeguarding policy and will be addressed through safeguarding procedures.

Chat Room Grooming and Offline Abuse

Our staff will need to be continually alert to any suspicious activity involving computers and the internet. Grooming of children online is a faster process than usual grooming, and totally anonymous. The abuser develops a 'special'

relationship with the child online (often adopting a false identity), which remains a secret to enable an offline meeting to occur for the abuser to harm the child.

---

18. Reporting Procedures

All breaches of the e-safety policy need to be recorded in the ICT reporting book that is kept in the general office. The details of the user, date and incident should be reported.

Accessible and Safe Reporting

Reporting procedures will be accessible to all students, including students with disabilities (alternative communication methods, accessible formats), EAL students (translation, simplified language), and students with communication difficulties (visual reporting tools, support from trusted adults).

The school recognizes that students experiencing identity-based cyber-bullying (racist, homophobic, transphobic, ableist, Islamophobic, sexist) may face barriers to reporting including fear of not being believed, fear of being outed, or mistrust of systems. Reporting procedures will be trauma-informed, confidential, and sensitive to these concerns.

All reports of identity-based cyber-bullying will be taken seriously and will be addressed through safeguarding procedures. Students will be supported and protected, and confidentiality will be maintained where appropriate.

Multiple Reporting Methods

Students can report online safety concerns through:

- Speaking to a trusted member of staff
- Written report (including anonymous reports)
- CEOP button for reporting online sexual abuse
- Childline
- Visual reporting tools (for students with communication difficulties)
- Email to the e-Safety Coordinator
- Through a parent/carer

Escalation Procedures

Child Protection Issues: Incidents which may lead to child protection issues need to be passed on to the Designated Safeguarding Lead immediately – it is their responsibility to decide on appropriate action.

Identity-Based Cyber-Bullying: All incidents of identity-based cyber-bullying (racist, homophobic, transphobic, ableist, Islamophobic, sexist, pregnancy-related) will be reported to the Designated Safeguarding Lead and treated as safeguarding concerns. Hate incidents will be reported to appropriate authorities.

Online Outing: Any incident of online outing (revealing a student's sexual orientation or gender identity without consent) will be treated as an urgent safeguarding concern and reported to the Designated Safeguarding Lead immediately.

Image-Based Sexual Abuse: Any incident involving sharing of intimate images without consent will be reported to the Designated Safeguarding Lead, police, and CEOP where appropriate.

Other Incidents: Incidents which are not child protection issues but may require Head Teacher intervention should be reported to the Head Teacher on the same day.

Staff Allegations: Allegations involving staff should be reported to the Headteacher. If the allegation is one of abuse, then it should be handled according to the DfE document titled 'Dealing with allegations of abuse against teachers and other staff'. If necessary, the local authority's LADO should be informed.

Evidence of incidents must be preserved and retained.

The curriculum will cover how pupils should report incidents (e.g. CEOP button, trusted adult, Childline).

---

19. Education

19.1 Pupils

To equip pupils as confident and safe users of ICT the school will undertake to provide:

a) A planned, broad and progressive e-safety education programme that is fully embedded for all children, in all aspects of the curriculum, in all years

b) Regularly auditing, review and revision of the ICT curriculum

c) E-safety resources that are varied and appropriate and use new technologies to deliver e-safety messages in an engaging and relevant manner

d) Opportunities for pupils to be involved in e-safety education e.g. through peer mentoring, e-safety committee, parent presentations

Additionally:

a) Pupils are taught in all lessons to be critically aware of the materials/content they access on-line and are guided to validate the accuracy of information

b) There are many opportunities for pupils to develop a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

c) The school actively provides systematic opportunities for pupils/students to develop the skills of safe and discriminating on-line behaviour

d) Pupils are taught to acknowledge copyright and intellectual property rights in all their work

19.2 Inclusive and Comprehensive E-Safety Education

E-safety education will be inclusive and address the diverse online safety needs of all students, including:

LGBTQ+-Specific Online Risks:

- Homophobic, biphobic, and transphobic cyber-bullying
- Online outing and how to protect privacy
- Targeted harassment
- How to access safe online spaces and LGBTQ+-affirming support
- Being an upstander against homophobic, biphobic, and transphobic cyber-bullying

Online Racism:

- Recognizing racist cyber-bullying and online hate speech
- How to respond to racist content
- Being an upstander against online racism
- Understanding racial microaggressions online

Disability-Based Cyber-Bullying:

- Recognizing ableist language and harassment
- Understanding that disability-based bullying is never acceptable
- How to report disability-based cyber-bullying
- Being an upstander against ableist cyber-bullying

Gender-Specific Online Risks:

- Online sexual harassment and how to respond
- Image-based sexual abuse and the law
- Consent and healthy relationships online
- Risks of sharing intimate images
- How to recognize and report online grooming
- Gender-based cyber-bullying (slut-shaming, appearance-based bullying)
- Pressure to share sexual images and how to resist

Religiously Motivated Cyber-Bullying:

- Recognizing Islamophobic, anti-Semitic, and other religious harassment
- How to respond to religiously motivated cyber-bullying
- Being an upstander against religious harassment

Identity-Based Cyber-Bullying:

- Understanding that targeting people based on protected characteristics is serious
- How to be an upstander against all forms of identity-based cyber-bullying
- Challenging stereotypes and promoting equality online

Online Hate Speech and Extremism:

- Recognizing extremist content and radicalization tactics
- How to report concerns about radicalization
- Critical thinking about online content

19.3 Accessible E-Safety Education

E-safety education will be accessible to all students, with adaptations for students with learning disabilities (simplified language, visual supports,

concrete examples), EAL students (accessible language, translation where needed), and students with communication difficulties.

Teaching materials will:

- Use diverse scenarios and examples that represent all students
- Be available in multiple formats (written, visual, audio)
- Use clear, accessible language
- Include concrete examples relevant to students' experiences
- Challenge stereotypes and promote equality

19.4 Staff Training

a) A planned programme of formal e-safety training is made available to all staff

b) E-safety training is an integral part of Child Protection/Safeguarding training and vice versa

c) An audit of e-safety training needs is carried out regularly and is addressed

d) All staff have an up-to-date awareness of e-safety matters, the current school e-safety policy and practices and child protection/safeguarding procedures

e) All new staff receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policy

f) Staff are encouraged to undertake additional e-safety training such as CEOP training or the European Pedagogical ICT Licence (EPICT) E-Safety Certificate

g) The culture of the school ensures that staff support each other in sharing knowledge and good practice about e-safety

h) The school takes every opportunity to research and understand good practice that is taking place in other schools

i) Governors are offered the opportunity to undertake training

19.5 Equality and Online Safety Training for Staff

All staff will receive training on equality, diversity, and online safety, including:

- Recognizing and responding to identity-based cyber-bullying (racist, homophobic, biphobic, transphobic, ableist, Islamophobic, sexist, pregnancy-related)
- Supporting LGBTQ+ students online, including understanding online outing and correct use of names/pronouns
- Supporting disabled students online, including understanding accessibility needs and disability-based cyber-bullying
- Cultural competence in online contexts
- Addressing unconscious bias in monitoring and sanctioning online behaviour
- Recognizing gender-specific online risks (online sexual harassment, image-based sexual abuse)
- Recognizing online grooming and sexual exploitation
- How to make ICT systems and e-safety education accessible
- Responding sensitively to reports from vulnerable students

---

20. Infringements and Sanctions

Whenever a student or staff member infringes the e-Safety Policy, the final decision on the level of sanction will be at the discretion of the Head Teacher.

Fair Application of Sanctions

Sanctions will be applied fairly and proportionately, taking into account individual circumstances, disabilities, communication difficulties, and cultural differences. The school will monitor whether certain groups of students are disproportionately sanctioned and will address any bias in sanctioning practices.

When applying sanctions, staff will consider whether online behaviour is related to disability (e.g., autistic students may struggle with social communication online), communication difficulties, or cultural differences in online communication. Reasonable adjustments will be made where appropriate.

Students who access LGBTQ+ support resources, anti-racism resources, or other educational content will not be sanctioned. The school recognizes the difference between accessing harmful content and accessing legitimate educational or support resources.

Important: Disability or health conditions will never be confused with breach of this policy. Sanctions will take account of disability-related online behaviour and will not penalize students for difficulties arising from their disability.

Students - Levels of Infringement

The following are provided as exemplification only:

Level 1 Infringements:

- Use of non-educational sites during lessons
- Unauthorised use of email
- Unauthorised use of mobile phone (or other new technologies) in lessons
- Use of unauthorised instant messaging/social networking sites

[Possible Sanctions: referred to class teacher/e-Safety Coordinator/confiscation of phone]

Level 2 Infringements:

- 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/social networking sites
- Use of file-sharing software
- Accidentally corrupting or destroying others' data without notifying a member of staff
- Accidentally accessing offensive material and not notifying a member of staff

[Possible Sanctions: referred to class teacher/e-safety Coordinator/removal of Internet access rights for a period/confiscation of phone/contact with parent]

Level 3 Infringements:

- Deliberately corrupting or destroying someone's data, violating privacy of others

- Sending an email or message that is regarded as harassment or of a bullying nature (one-off)
- Deliberately trying to access offensive or pornographic material

[Possible Sanctions: referred to class teacher/e-safety Coordinator/Headteacher/removal of Internet rights for a period/contact with parents/carers]

Other safeguarding actions: If inappropriate web material is accessed:

1. Ensure appropriate technical support filters the site
2. Inform SSCP/LA as appropriate

Level 4 Infringements:

- Continued sending of emails or messages regarded as harassment or of a bullying nature after being warned
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic, biphobic, transphobic, ableist, Islamophobic, sexist or violent
- Identity-based cyber-bullying (racist, homophobic, biphobic, transphobic, ableist, Islamophobic, sexist, pregnancy-related harassment)
- Online outing (revealing someone's sexual orientation or gender identity without consent)
- Sharing of intimate images without consent
- Sharing of pre-transition images without consent
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act
- Bringing the school's name into disrepute

[Possible Sanctions: Referred to Head Teacher/Contact with parents/possible suspension/referral to Community Police Officer/LA e-safety officer/police/CEOP where appropriate]

Other safeguarding actions:

1. Secure and preserve any evidence
2. Inform the sender's e-mail service provider if a system other than the school system is used
3. Report hate incidents to appropriate authorities

4. Report to police and CEOP where appropriate (e.g., image-based sexual abuse, online sexual exploitation)

Pupils are also informed that sanctions can be applied to e-safety incidents that take place out of school if they are related to school.

Staff - Levels of Infringement

Level 1 Infringements (Misconduct):

- Excessive use of Internet for personal activities not related to professional development
- Misuse of first level data security, e.g. wrongful use of passwords
- Breaching copyright or license e.g. installing unlicensed software on network

[Sanction: Headteacher. Warning given.]

Level 2 Infringements (Gross Misconduct):

- Serious misuse of, or deliberate damage to, any school computer hardware or software
- Any deliberate attempt to breach data protection or computer security rules
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic, biphobic, transphobic, ableist, Islamophobic, sexist or violent
- Discrimination, harassment or victimisation based on protected characteristics online
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act
- Bringing the school's name into disrepute

[Sanction: Referred to Headteacher/Governors and follow school disciplinary procedures; report to LA Personnel/Human resources, report to Police/TRA/DfE]

Other safeguarding actions:

1. Remove the PC to a secure place to ensure that there is no further access
2. Instigate an audit of all ICT equipment by an outside agency
3. Identify the precise details of the material

If a member of staff commits an exceptionally serious act of gross misconduct, they 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 Human Resources team.

---

21. Rewards

Whilst recognising the need for sanctions it is important to balance these with rewards for positive reinforcement. The rewards can take a variety of forms – e.g. class commendation for good research skills, certificates for being good cyber citizens, recognition for being an upstander against cyber-bullying, etc.

Students will be recognised and rewarded for:

- Responsible and respectful online behaviour
- Being an upstander against cyber-bullying and online discrimination
- Supporting peers experiencing online difficulties
- Demonstrating good digital citizenship
- Challenging stereotypes and promoting equality online

Each year teachers will indicate these opportunities within the provided planning.

---

22. Monitoring and Review

22.1 Policy Review

The e-Safety Policy and its implementation will be reviewed annually by the e-Safety Coordinator, SENDCo, Designated Safeguarding Lead, and a governor with responsibility for e-safety.

The school will audit use of technology to establish if the e-safety policy is adequate and appropriately implemented. Methods to identify, assess and minimise risks will be reviewed annually.

22.2 Equality Monitoring

The school will monitor online safety incidents by type (including identity-based cyber-bullying: racist, homophobic, biphobic, transphobic, ableist, Islamophobic, sexist, pregnancy-related) and by protected characteristics of victims and perpetrators where appropriate and in compliance with data protection regulations.

The school will monitor whether certain groups of students are disproportionately affected by cyber-bullying or disproportionately sanctioned for online behaviour.

Monitoring data will be reported to governors annually and will be used to identify and address any disparities in online safety outcomes or sanctioning practices.

22.3 Student Voice

Student voice on online safety will include students from diverse backgrounds to ensure their experiences and needs are understood. The school will:

- Conduct regular student voice surveys on online safety (disaggregated by protected characteristics where appropriate and with data protection)
- Consult with students from diverse backgrounds about their online safety experiences
- Include student representatives in the e-safety committee
- Act on feedback to improve inclusivity and effectiveness

22.4 Reporting to Governors

The e-Safety Coordinator will provide an annual report to governors including:

- Overview of online safety incidents and trends
- Equality monitoring data (anonymized and aggregated)
- Analysis of any disparities in cyber-bullying victimization or sanctioning
- Actions taken to address identified issues
- Effectiveness of e-safety education
- ICT accessibility audit findings
- Filtering system review
- Staff training completion rates
- Student voice feedback

- Recommendations for policy and practice improvements

22.5 Accessibility Audit

The school will conduct an annual audit of ICT systems for accessibility, including:

- Review of assistive technology provision
- Assessment of whether all students can access ICT systems effectively
- Identification of barriers for disabled students
- Review of reasonable adjustments in place
- Consultation with disabled students and the SENDCo
- Action plan to address any identified barriers

22.6 Filtering System Review

The school will conduct an annual review of filtering systems to ensure:

- Hate content (racist, homophobic, biphobic, transphobic, ableist, Islamophobic, extremist) is effectively blocked
- Legitimate LGBTQ+ support resources, mental health support, and educational content are not blocked
- Students can request access to blocked resources through a clear process
- Filtering is applied fairly without targeting specific groups

---

23. Agreement

All school employees, contractors or temporary staff who have been granted the right to use the school's internet access are required to sign this agreement confirming their understanding and acceptance of this policy.

I confirm that I have read, understood, and agree to comply with the Acceptable Use of Information Technology, Online Safety and Cyber-Abuse Policy, including:

- The commitment to equality and inclusion in online contexts
- The requirement to make reasonable adjustments for disabled students
- The prohibition on all forms of identity-based discrimination and harassment online

- The fair and non-discriminatory application of monitoring and sanctions
- The procedures for reporting online safety concerns, including identity-based cyber-bullying
- The responsibility to model inclusive, respectful online conduct
- The commitment to challenging discrimination and supporting all students online

I understand that breaches of this policy may result in disciplinary action.

Name (print): _____

Signature: _____ **Date:** _____

Signatures:	
Headteacher:	
Chair of Governors:	