E-Safety (including Acceptable Use) Policy

Contents	Page(s)
1. Introduction and legislation	2-3
2. Scope	3-4
3. Equality and diversity in online safety	4-7
4. Securely maintaining information	7-8
5. Roles and responsibilities	8-10
6. Curriculum	10-14
7. Training	14-15
8. Use of IT facilities for teaching and learning	15
9. GDPR and online safety	15-16
10. Monitoring	16-17
11. Appendices	17-23

Postholder responsible: Domoni Supple	**Date:** 20/07/2022
Last reviewed on: 02/03/2026, 22/06/2026	

Postholder responsible: Domoni Supple	**Date:** 20/07/2022
Next review due by: 02/06/2029	

1. Introduction and legislation

The Physis Academy E-Safety policy aims to create an environment where pupils, staff, parents/carers, governors, and the wider school community work together to inform each other of ways to use the Internet responsibly, safely, and positively.

Through teaching ICT, we equip children and young people to participate in a rapidly changing world where work and leisure activities are increasingly transformed by technology. We enable them to find, explore, analyse, exchange and present information in a varied and stimulating way. ICT skills are a major factor in enabling them to be confident, creative, and independent learners. As the aims of ICT are to equip children and young people with the skills necessary to use technology to become independent learners, the teaching style that we adopt is as active and practical as possible. We provide suitable learning opportunities for all children and young people by matching the challenge of the task to the ability and experience of the child or young person. Internet technology helps pupils learn creatively and effectively and encourages collaborative learning and the sharing of good practice amongst all school stakeholders.

The E-Safety policy encourages appropriate and safe conduct and behaviour when achieving this. Pupils, staff and all other users of school related technologies will work together to agree standards and expectations relating to usage in order to promote and ensure good behaviour. These agreements and their implementation will promote positive behaviour which can transfer directly into each pupil's adult life and prepare them for experiences and expectations in the workplace. The policy is not designed to be a list of prohibited activities, but instead a list of areas to discuss, teach and inform, in order to develop positive behaviour and knowledge leading to safer Internet usage and year on year improvement and measurable impact on online safety. It is intended that the positive effects of the policy will be seen online and offline; in school and at home; and ultimately beyond school and into the workplace.

Equality and Non-Discrimination

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 spaces
- Advancing equality of opportunity for all users of technology

- Fostering good relations through inclusive digital practices

We recognize that online experiences and risks vary across protected characteristics (age, disability, gender reassignment, pregnancy and maternity, race, religion or belief, sex, and sexual orientation). This policy ensures that our online safety provisions are sensitive to the needs of all members of our school community and that technology is used to promote equality and celebrate diversity.

This online safety policy is developed using the following legislation:

- The Education and Inspections Act 2006 (Headteachers have the power "to such an extent as is reasonable" to regulate the conduct of pupils off site)
- Computer Misuse Act 1990, sections 1-3
- Data Protection Act 2018
- UK General Data Protection Regulation (UK GDPR)
- Freedom of Information Act 2000
- Communications Act 2003 sections 1, 2
- Protection from Harassment Act 1997
- Regulation of Investigatory Powers Act 2000
- Copyright, Designs and Patents Act 1988
- Racial and Religious Hatred Act 2006
- Protection of Children Act 1978
- Sexual Offences Act 2003
- Equality Act 2010
- Keeping Children Safe in Education (2023)
- Prevent Duty Guidance (2023)
- Online Safety Act 2023

Schools have a 'duty of care' to pupils, and as such act "in loco parentis." Under the Children Act 1989, this enables schools to remove personal information, cyber bullying and comments relating to pupils, as if they were the child's parent/carer. Social media platforms have provision for using 'in loco parentis' when reporting cyber bullying. This is relevant to all schools.

---

2. Scope

The academy E-Safety policy and agreements apply to all pupils, staff, support staff, external contractors and members of the wider school community who use, have access to or maintain school and school related Internet, computer systems and mobile technologies internally and externally.

The school will make reasonable use of relevant legislation and guidelines to affect positive behaviour regarding ICT and Internet usage both on and off the school site. 'In Loco Parentis' provision under the Children Act 1989 also allows the school to report and act on instances of cyber bullying, abuse, harassment (including sexual harassment), malicious communication and grossly offensive material, including reporting to the police, social media websites, and hosting providers on behalf of pupils.

The E-Safety policy covers the use of:

- School based ICT systems and equipment
- School based intranet and networking
- School related external Internet, including but not exclusively, extranet, e-learning platforms, blogs, social media websites
- External access to internal school networking, such as webmail, network access, file-serving (document folders) and printing
- School ICT equipment off-site, for example staff laptops, digital cameras, mobile phones, tablets
- Pupil and staff personal ICT equipment when used in school and which makes use of school networking, file-serving, or Internet facilities
- Tablets, mobile phones, devices, and laptops when used on the school site
- Management Information Systems
- MP3 players and other digital devices
- Assistive technologies used by pupils with disabilities
- Communication aids and alternative access devices

This policy applies to all members of the school community:

Pupils: The policy recognizes that pupils aged 11-18 have different levels of digital maturity and face age-specific online risks. Online safety teaching and supervision will be appropriately differentiated.

Staff: All staff, regardless of role, are expected to model positive online behaviour and maintain professional standards in all digital communications.

Parents/carers and families: The school will work in partnership with families from diverse backgrounds, providing accessible information and support.

Governors and trustees: Governors have oversight responsibility for online safety and equality compliance.

Visitors and contractors: All users of school systems must agree to acceptable use standards.

---

3. Equality and diversity in online safety

Recognition of Protected Characteristics

The school recognizes that online experiences, risks, and access to technology vary significantly across protected characteristics. This policy ensures that all members of our school community are protected from online harm and can benefit equally from technology.

Age

Pupils aged 11-18:

- The school serves pupils across early adolescence (11-13), mid-adolescence (14-16), and late adolescence (17-18)
- Online safety teaching is differentiated to be age-appropriate and developmentally sensitive
- Younger pupils may require more supervision and scaffolding; older pupils need guidance on managing increasing online independence
- Age-specific risks are addressed (e.g., early adolescents and peer pressure online; older pupils and online reputation for future employment/education)
- Filtering and monitoring are adjusted appropriately for different age groups while maintaining safety

Staff:

- All staff receive online safety training regardless of age or digital confidence
- Support is available for staff who may be less familiar with emerging technologies

Disability

Pupils with disabilities and SEND:

The school recognizes that:

- Pupils with disabilities may face increased online risks including exploitation, bullying, and isolation
- Assistive technologies must be secured appropriately while maintaining accessibility
- Online safety teaching must be accessible to all pupils regardless of learning needs
- Communication about online safety must be adapted for pupils with communication disabilities

Provisions:

- All online safety materials are available in accessible formats (easy read, visual supports, audio versions, large print)
- Teaching is differentiated for pupils with learning disabilities using simplified language, concrete examples, and visual supports
- Alternative communication methods are available for reporting concerns (visual tools, communication apps, non-verbal options)
- Assistive technologies are secured and monitored appropriately without compromising accessibility
- Staff are trained on online safety risks specific to disabled pupils
- Filtering is reviewed to ensure it doesn't block legitimate disability-related resources
- Reasonable adjustments are made to ensure equal access to online learning
- Sensory needs are considered in the use of technology (screen brightness, sound levels, etc.)

Gender Reassignment

Transgender and gender-questioning pupils:

The school recognizes that:

- Transgender pupils face significantly elevated online risks including transphobic bullying, misgendering, deadnaming, and outing
- Online spaces may be where pupils first explore gender identity
- Privacy and confidentiality are critical

Provisions:

- Transphobic content and behaviour are explicitly prohibited and will be addressed immediately
- Digital systems respect pupils' chosen names and pronouns
- Privacy settings protect pupils who are exploring or transitioning gender identity
- Staff are trained to recognize and respond to transphobic online bullying
- Filtering ensures safe access to age-appropriate, evidence-based information about gender identity
- Reporting mechanisms protect confidentiality
- Online safety teaching includes content on respectful discourse about gender identity

Pregnancy and Maternity

Pregnant pupils and young mothers:

The school recognizes that:

- Pregnant pupils and young mothers may face online harassment, shaming, or sharing of images without consent
- They require continued access to online learning during medical appointments or maternity leave

Provisions:

- Pregnancy-related bullying and harassment are explicitly prohibited
- Privacy and dignity are protected in all digital communications
- Flexible access to online learning is ensured
- Safe access to age-appropriate information about pregnancy and parenting is provided
- Staff are trained to recognize and address pregnancy-related online harassment

Race and Ethnicity

Pupils from minoritized ethnic backgrounds:

The school recognizes that:

- Pupils from minoritized ethnic backgrounds may experience online racism, racial harassment, and hate speech
- Cultural and linguistic diversity must be reflected in online safety provision

- Filtering and monitoring must not discriminate

Provisions:

- Racist content, language, symbols, and hate speech are explicitly prohibited and proactively monitored
- Clear reporting pathways exist for racist incidents with appropriate consequences
- Support is provided for victims of online racism
- Online safety materials represent diverse racial and ethnic backgrounds
- Staff are trained to recognize and address online racism including microaggressions
- Filtering is reviewed to ensure it doesn't inappropriately block legitimate cultural or language-specific content
- Information is available in multiple languages where needed
- Cultural sensitivity is maintained in all digital communications

Religion or Belief

Pupils of all faiths and none:

The school recognizes that:

- Pupils may face religious discrimination, harassment, or hate speech online
- Radicalisation concerns must be balanced with respect for religious freedom
- Filtering must not inappropriately block legitimate religious content

Provisions:

- Religious hate speech and discrimination are explicitly prohibited
- Filtering is reviewed to ensure it doesn't inappropriately block legitimate religious content while blocking extremist material
- Radicalisation concerns are addressed sensitively and proportionately
- Online safety teaching includes respectful discourse about diverse beliefs
- Staff are trained to recognize religious discrimination while maintaining appropriate safeguarding vigilance
- Support is available for pupils experiencing religious conflict or pressure

Sex

All pupils:

The school recognizes that:

- Girls and boys may face different gender-specific online risks
- Girls face higher risks of sexual harassment, image-based abuse, and misogyny online
- Boys face higher risks of exposure to violent content and criminal exploitation
- Both face risks of gender-based violence and harmful gender stereotypes

Provisions:

- Sexual harassment, misogyny, sexism, and gender-based harassment are explicitly prohibited
- Image-based abuse and non-consensual sharing of images are addressed with clear procedures
- Online safety teaching addresses gender stereotypes, consent, and respectful relationships
- Staff are trained to recognize and address gender-based online violence
- Monitoring captures sex-disaggregated data on online safety incidents
- Equal access and participation in online learning is ensured for all genders

Sexual Orientation

LGBTQ+ pupils:

The school recognizes that:

- LGBTQ+ pupils face significantly elevated online risks including homophobic, biphobic bullying, harassment, and hate speech
- Online spaces may be where pupils first explore sexual orientation
- Privacy and confidentiality are critical to prevent outing

Provisions:

- Homophobic, biphobic, and other LGBTQ+-related hate speech and bullying are explicitly prohibited
- Clear reporting pathways exist with appropriate consequences
- Privacy is protected to prevent outing

- Filtering ensures safe access to age-appropriate, evidence-based LGBTQ+ support resources and information
- Online safety teaching includes respectful discourse about diverse sexual orientations
- Staff are trained to recognize and respond to LGBTQ+-related online bullying
- Support is provided for pupils experiencing family rejection or conflict related to sexual orientation

Intersectionality

The school recognizes that pupils may hold multiple protected characteristics and face compounded online risks. For example:

- LGBTQ+ pupils from minoritized ethnic backgrounds may face both racism and homophobia
- Disabled LGBTQ+ pupils may face both ableism and LGBTQ+-related discrimination
- Transgender pupils from religious backgrounds may experience conflict between identity and faith

Online safety provision addresses pupils' whole identities and intersecting experiences.

Positive Use of Technology for Equality

The school promotes the positive use of technology to:

- Celebrate diversity and connect with communities
- Access support and information related to protected characteristics
- Challenge discrimination and promote equality
- Develop digital citizenship that includes respect for all

---

4. Securely maintaining information

It is important to review the security of the whole system from user to Internet. This is a major responsibility that includes not only the delivery of essential learning services but also the personal safety of staff and pupils.

Local network security issues include:

- Users must act reasonably — e.g., the downloading of large files during the working day will affect the service that others receive

- Users must take responsibility for their network use
- Workstations should be secured against user mistakes and deliberate actions
- Virus protection for the whole network must be installed and current
- Access by wireless devices must be proactively managed and secured

Wider network security issues include:

- The security of the school information systems and users will be reviewed regularly
- Virus protection will be updated regularly
- Personal data sent over the Internet or taken off site will be encrypted
- Portable media may not be used unless it has been encrypted and virus checked
- Unapproved software will not be allowed in work areas or attached to email
- The use of user logins and passwords to access the network will be enforced
- Particular care will be taken with data relating to protected characteristics to ensure compliance with the Equality Act 2010 and data protection legislation

Filter management:

- The school's broadband access provides filtering appropriate to the age and maturity of pupils
- There is flexibility in the filtering system to allow for changes in provision depending on the learning required
- The school filtering system will block all sites on the Internet Watch Foundation (IWF) list
- Filtering will block hate sites targeting all protected characteristics (racist, homophobic, transphobic, ableist, sexist, religiously discriminatory content)
- Changes to the school filtering policy will be risk assessed by staff with educational and technical experience prior to any changes and where appropriate with consent from the Senior Leadership Team
- **Filtering will be regularly reviewed through an equality lens to ensure it:**
    - Does not inappropriately block legitimate content related to protected characteristics (e.g., LGBTQ+ support sites, disability resources, cultural or religious content, age-appropriate sex education)
    - Effectively blocks discriminatory, hateful, and harmful content

    - Provides appropriate access to support resources for pupils with protected characteristics

- The School Senior Leadership Team will ensure that regular checks are made to ensure that the filtering methods selected are effective and equitable
- A clear process exists for pupils and staff to request review of blocked sites
- Any material that the school believes is illegal will be reported to appropriate agencies

Equality considerations in monitoring:

- Monitoring will be proportionate and will not target pupils based on protected characteristics
- Privacy will be balanced with safeguarding, particularly for pupils exploring identity (gender identity, sexual orientation)
- Monitoring data will be reviewed to identify any disproportionate impact on pupils with protected characteristics

5. Roles and responsibilities

In the event of an online safety incident, the following people will be informed within school:

Headteacher	James Nation
Designated Safeguarding Lead (DSL)	James Nation
Deputy Designated Safeguarding Leads (DDSLs)	Domoni Supple, Katherine Mooney

Senior Leadership Team

The school senior leadership team is responsible for determining, evaluating, and reviewing E-Safety policies to encompass teaching and learning, use of school IT equipment and facilities by pupils, staff and visitors, and the agreed criteria for acceptable use by pupils, school staff and governors of Internet capable equipment for school related purposes or in situations which will impact on the reputation of the school, and/or on school premises.

The online safety policy is a result of a continuous cycle of evaluation and review based on new initiatives, partnership discussion with stakeholders and outside organisations, technological and Internet developments, current government guidance and school

related online safety incidents. The policy development cycle develops good practice within the teaching curriculum and wider pastoral curriculum. Regular assessment of strengths and weaknesses help determine INSET provision for staff and governors and guidance provided to parents, pupils, and local partnerships.

Online safety provision is always designed to encourage positive behaviours and practical real-world strategies for all members of the school and wider school community, with explicit recognition of how protected characteristics affect online experiences and risks.

The leadership team is encouraged to be aspirational and innovative in developing strategies for online safety provision that promote equality and celebrate diversity.

Teachers and support staff

Teaching and support staff need to ensure that they are aware of the current school online safety policy, practices, and associated procedures for reporting online safety incidents.

Teaching and support staff will be provided with online safety training, including training on equality, diversity, and online safety.

All staff need to ensure that they have read, understood, and signed (thereby indicating agreement) the Acceptable Use Agreement relevant to Internet and computer use in school.

All staff need to follow the school's social media policy, regarding external off-site use, personal use (mindful of not bringing the school into disrepute), possible contractual obligations, and conduct on Internet school messaging or communication platforms, for example email and forums.

All teaching staff need to rigorously monitor learner Internet and computer usage in line with the policy. This also includes the use of personal technology such as cameras, phones, and other gadgets on the school site.

Teaching staff should promote best practice regarding avoiding copyright infringement and plagiarism.

Staff should be aware of online propaganda and help pupils with critical evaluation of online materials, including discriminatory content.

Internet usage and suggested websites should be pre-vetted and documented in lesson planning.

Staff responsibilities regarding equality:

- Recognize and respond to online discrimination and hate speech across all protected characteristics

- Ensure online safety teaching is accessible to all pupils, including those with disabilities
- Respect pupils' protected characteristics in all digital communications
- Challenge discriminatory online behaviour and promote positive digital citizenship
- Report incidents of online discrimination through appropriate channels

Designated Safeguarding Lead

The Designated Safeguarding Lead is trained in specific online safety issues. Accredited training with reference to child protection issues has been accessed, including training on protected characteristics and online safety.

The Designated Safeguarding Lead can differentiate which online safety incidents are required to be reported to CEOP, local Police, Local Safeguarding Children Partnership, social services, and parents/carers; and also determine whether the information from such an incident should be restricted to nominated members of the leadership team.

Possible scenarios might include:

- Allegations against members of staff
- Computer crime – for example hacking of school systems
- Allegations or evidence of 'grooming'
- Allegations or evidence of cyber bullying in the form of threats of violence, harassment, or a malicious communication
- Producing and sharing of Youth Produced Sexual Imagery
- Online hate speech or discrimination based on protected characteristics
- Transphobic, homophobic, racist, or other discriminatory online bullying
- Outing of pupils' protected characteristics without consent

The DSL is responsible for acting 'in loco parentis' and liaising with websites and social media platforms such as Twitter, Instagram, Snapchat, TikTok, and Facebook to remove instances of illegal material, cyber bullying, or discriminatory content.

The DSL will ensure:

- Incidents involving protected characteristics are handled sensitively and appropriately
- Privacy is protected, particularly where outing could occur (e.g., LGBTQ+ pupils, pupils exploring gender identity)

- Support is provided for victims of online discrimination
- Appropriate agencies are involved where hate crimes have occurred

Pupils

Pupils are required to use school Internet and computer systems in agreement with the terms specified in the school Acceptable Use Policies. Pupils are expected to sign the policy to indicate agreement, and/or have their parents/carers sign on their behalf.

Pupils need to be aware of how to report online safety incidents in school, and how to use external reporting facilities, such as the Click CEOP button or Childline number. Reporting mechanisms are accessible to all pupils, including those with communication disabilities.

Pupils need to be aware that school Acceptable Use Policies cover all computer, Internet, and mobile technology usage in school, including the use of personal items such as phones.

Pupils need to be aware that their Internet use out of school on social networking sites such as Instagram, TikTok, and Snapchat is covered under the Acceptable Use Policy if it impacts on the school and/or its staff and pupils in terms of cyber bullying, reputation, or illegal activities.

Pupils are expected to:

- Treat others with respect online, regardless of protected characteristics
- Not engage in or share discriminatory, hateful, or offensive content
- Report incidents of online discrimination or bullying
- Understand that the same standards of behaviour apply online and offline

Parents/carers

It is hoped that parents/carers will support the school's stance on promoting good Internet behaviour and responsible use of IT equipment and mobile technologies both at school and at home.

The school will provide parents/carers with:

- Information about online safety in accessible formats
- Guidance on supporting their children's online safety at home
- Information in multiple languages where needed
- Support in understanding online risks specific to pupils with protected characteristics

Other users

Other users such as school visitors, or wider school community stakeholders or external contractors should be expected to agree to a visitor's Acceptable Use Agreement (AUA) document specific to their level of access and usage.

External users with significant access to school systems including sensitive information or information held securely under data protection legislation should be DBS checked. This includes external contractors who might maintain the school IT systems – which may facilitate access to cloud file storage, website documents, and email.

---

6. Curriculum

From September 2020, Relationships and Sex Education has been compulsory for all secondary aged pupils. Through these subjects, pupils are taught about online safety and harms. This includes being taught what positive, healthy and respectful online relationships look like, the effects of their online actions on others and knowing how to recognise and display respectful behaviour online. Throughout these subjects, teachers address online safety and appropriate behaviour in an age-appropriate way that is relevant to pupils' lives.

'Teaching online safety in school' (DfE, June 2019) outlines to schools the importance of helping children and young people not only use the internet safely but also give them opportunities to learn how to behave online. Throughout the compulsory Relationships and Sex Education and Health Education, pupils are taught what positive, healthy and respectful online relationships look like.

There are also other curriculum subjects which include content relevant to teaching pupils how to use the internet safely. For example, citizenship education covers media literacy - distinguishing fact from opinion as well as exploring freedom of speech and the role and responsibility of the media in informing and shaping public opinion. It also supports teaching about the concept of democracy, freedom, rights, and responsibilities.

PSHE curriculum underpinning knowledge and behaviours:

How to evaluate what they see online

This enables pupils to make judgements about what they see online and not automatically assume that what they see is true, valid or acceptable.

This includes:

- Is this website/URL/email fake? How can I tell?
- What does this cookie do and what information am I sharing?

- Is this person who they say they are?
- Why does someone want me to see this?
- Why does someone want me to send this?
- Why would someone want me to believe this?
- Why does this person want my personal information?
- What's behind this post?
- Is this too good to be true?
- Is this fact or opinion?
- Is this content discriminatory or hateful? How can I tell?
- Does this content stereotype or misrepresent people with protected characteristics?

How to recognise techniques used for persuasion

This enables pupils to recognise the techniques that are often used to persuade or manipulate others. Understanding that a strong grasp of knowledge across many areas makes people less vulnerable to these techniques and better equipped to recognise and respond appropriately to strongly biased intent or malicious activity.

This includes:

- Online content which tries to make people believe something false is true and/or mislead (misinformation and disinformation)
- Techniques that companies use to persuade people to buy something
- Ways in which games and social media companies try to keep users online longer (persuasive design)
- Criminal activities such as grooming
- How algorithms can reinforce stereotypes and discrimination
- How extremist groups use online platforms to recruit and radicalise

Online behaviour

This enables pupils to understand what acceptable and unacceptable online behaviour look like. Pupils are taught that the same standard of behaviour and honesty apply on and offline, including the importance of respect for others.

This includes:

- Looking at why people behave differently online, for example how anonymity (you do not know me) and invisibility (you cannot see me) affect what people do
- Looking at how online emotions can be intensified resulting in mob mentality
- Teaching techniques (relevant on and offline) to defuse or calm arguments, for example a disagreement with friends, and disengage from unwanted contact or content online
- Considering unacceptable online behaviours often passed off as so-called social norms or just banter. For example, negative language that can be used, and in some cases is often expected, as part of online gaming and the acceptance of misogynistic, homophobic, biphobic, transphobic, racist, ableist, and other discriminatory language that would never be tolerated offline
- Understanding that discrimination, hate speech, and harassment online are never acceptable
- Recognizing the impact of online discrimination on mental health and wellbeing
- Being an active ally and challenging discrimination online

How to identify online risks

This enables pupils to identify possible online risks and make informed decisions about how to act. This should not be about providing a list of what not to do online. The focus should be to help pupils assess a situation, think through the consequences of acting in different ways and decide on the best course of action.

Schools help pupils to identify and manage risk by:

- Discussing the ways in which someone may put themselves at risk online
- Discussing risks posed by another person's online behaviour
- Discussing when risk taking can be positive and negative
- Discussing "online reputation" and the positive and negative aspects of an online digital footprint. This could include longer-term considerations, i.e., how past online behaviours could impact on their future, when applying for a place at university or a job for example
- Discussing the risks vs. the benefits of sharing information online and how to make a judgement about when and how to share and who to share with
- Asking questions such as what might happen if I post something online? Who will see it? Who might they send it to?

- Understanding specific online risks related to protected characteristics (e.g., outing, hate speech, targeted harassment)
- Recognizing that pupils with certain protected characteristics may face elevated online risks

How and when to seek support

This enables pupils to understand safe ways in which to seek support if they are concerned or upset by something they have seen online. Pupils will understand how to:

- Identify who trusted adults are
- Look at different ways to access support from the school, police, the National Crime Agency's Click CEOP reporting service for children and young people, and 3rd sector organisations such as Childline and Internet Watch Foundation. This should link to wider school policies and processes around reporting of safeguarding and child protection incidents and concerns to school staff (see KCSIE)
- Help them to understand that various platforms and apps will have ways in which inappropriate contact or content can be reported
- Access specialist support services related to protected characteristics (e.g., LGBTQ+ support organizations, anti-racism organizations, disability advocacy groups)
- Report hate crimes and discrimination to appropriate authorities
- Use accessible reporting methods appropriate to their communication needs

Teaching about potential harms

Throughout the curriculum teaching about potential harms will include, following consultation and agreement with parents/carers, social workers (where applicable) and Physis Group Clinical Services:

Technical risks:

- Age restrictions
- Content: How it can be used and shared
- Disinformation, misinformation, and hoaxes
- Fake websites and scam emails
- Fraud (online)
- Password phishing

- Personal data
- Persuasive design which keeps 'users online for longer than they might have planned or desired'
- Privacy settings
- Targeting of online content

Content risks:

- Abuse (online)
- Challenges [to do something and post about it]
- Content which incites hate, violence
- Discriminatory content (racist, sexist, homophobic, biphobic, transphobic, ableist, religiously discriminatory)
- Fake profiles
- Grooming
- Live streaming
- Pornography
- Unsafe communication
- Extremist and radicalisation content

Contact risks:

- Cyberbullying, including bullying based on protected characteristics
- Hate speech and harassment
- Outing (sharing someone's protected characteristic without consent)
- Misgendering and deadnaming
- Sexual harassment and image-based abuse

Wellbeing risks:

- Impact on confidence (including body confidence)
- Impact on quality of life, physical and mental health, and relationships
- Online vs. offline behaviours
- Reputational damage
- Suicide, self-harm and eating disorders

- Impact of discrimination and minority stress on mental health

Equality and diversity in online safety teaching

The school ensures that online safety teaching:

- Is accessible to all pupils, including those with learning disabilities (using simplified language, visual supports, concrete examples)
- Represents diverse pupils in examples and case studies
- Explicitly addresses discrimination across all protected characteristics
- Teaches pupils to celebrate diversity online and be active allies
- Addresses how algorithms and platforms can perpetuate discrimination
- Provides age-appropriate, evidence-based information about protected characteristics
- Is culturally sensitive and religiously inclusive
- Challenges stereotypes and promotes positive representations

Specific content includes:

- **LGBTQ+ online safety:** Understanding homophobia, biphobia, and transphobia online; safe access to LGBTQ+ support; privacy and outing; being an ally
- **Race and online safety:** Understanding racism online including microaggressions; challenging racist content; celebrating cultural diversity
- **Disability and online safety:** Understanding ableism; accessibility; challenging stereotypes
- **Gender and online safety:** Understanding misogyny and sexism; consent and image-based abuse; challenging gender stereotypes
- **Religion and online safety:** Understanding religious discrimination; respectful discourse about diverse beliefs; recognizing extremism while respecting faith

Online safety is accessed as part of tutor time activities and assemblies as well as online safety events – such as Safer Internet Day and Anti-Bullying Week.

---

7. Training

A programme of online safety training opportunities is available for staff including:

- Whole staff training

- Online training opportunities (for example Online Safety Support courses)
- External CPD courses, accredited CPD courses (for example CEOP) and Coordinator training

Equality and diversity in online safety training

All online safety training includes comprehensive coverage of equality, diversity, and online safety, including:

Protected characteristics and online safety risks:

- Understanding how protected characteristics affect online experiences and risks
- Recognizing specific risks for:
    - LGBTQ+ pupils (family rejection, mental health, bullying, outing)
    - Transgender pupils (gender dysphoria, family conflict, transphobia, misgendering, deadnaming)
    - Pupils from minoritized ethnic backgrounds (racism, cultural dislocation, hate speech)
    - Disabled pupils (communication barriers, increased vulnerability to exploitation, accessibility)
    - Pregnant pupils and young mothers (harassment, shaming, stigma)
    - Pupils experiencing religious conflict or persecution

Recognizing and responding to online discrimination:

- Identifying hate speech across all protected characteristics
- Understanding the difference between banter and discrimination
- Recognizing microaggressions and subtle forms of discrimination
- Understanding intersectional discrimination
- Appropriate, sensitive responses to incidents affecting pupils with protected characteristics

Cultural competence:

- Understanding cultural differences in online behaviour and communication
- Recognizing how cultural background affects online experiences
- Avoiding cultural stereotyping
- Working sensitively with diverse families

LGBTQ+ awareness:

- Understanding extremely high mental health risks for LGBTQ+ pupils
- Recognizing signs of family rejection or conflict
- Providing LGBTQ+-affirming support
- Managing confidentiality when family relationships are strained
- Understanding the importance of privacy to prevent outing

Disability awareness:

- Adapting communication for pupils with disabilities
- Understanding specific vulnerabilities when disabled pupils go missing
- Making reasonable adjustments in online safety provision
- Ensuring accessibility of online safety materials and reporting mechanisms

Unconscious bias:

- Recognizing unconscious bias in online safety responses
- Avoiding stereotyping based on protected characteristics
- Ensuring equitable treatment for all pupils
- Understanding how bias affects filtering and monitoring decisions

Legal duties:

- Understanding the Equality Act 2010 and Public Sector Equality Duty
- Recognizing when online incidents constitute hate crimes
- Understanding data protection in relation to protected characteristics
- Knowing when to involve specialist agencies

Specialist training

The DSL, DDSLs, and senior leaders receive specialist training on:

- Advanced safeguarding for pupils with protected characteristics
- Cultural competence in safeguarding
- LGBTQ+ safeguarding
- Working with diverse families
- Legal duties under the Equality Act 2010

- Hate crime recognition and reporting

Ongoing professional development

Staff receive regular updates on:

- Emerging online risks affecting pupils with protected characteristics
- New platforms and technologies
- Changes to legislation and guidance
- Best practice in inclusive online safety provision

8. Use of IT facilities for teaching and learning

Use of the Internet and IT facilities should be clearly planned prior to the activity. Websites and software Apps should be suggested, pupils should be trusted to be responsible when researching the Internet however, internet usage should always be supervised for pupils at Physis Academy unless advised otherwise. Teaching staff will consider the age and maturity of the pupils when setting online learning tasks.

Staff will ensure that:

- Online learning is accessible to all pupils, including those with disabilities
- Assistive technologies are available and properly secured
- Alternative formats are provided where needed (visual, audio, simplified text)
- Online tasks do not inadvertently discriminate against pupils with protected characteristics
- Equal access to technology and online learning is maintained for all pupils

---

9. GDPR and online safety

The UK GDPR sets out the key principles that all personal data must be processed in line with.

Data must be processed lawfully, fairly, and transparently; collected for specific, explicit and legitimate purposes; limited to what is necessary for the purposes for which it is processed; accurate and kept up to date; held securely; only retained for as long as is necessary for the reasons it was collected.

There are also stronger rights for individuals regarding their own data.

The individual's rights include: to be informed about how their data is used, to have access to their data, to rectify incorrect information, to have their data erased, to

restrict how their data is used, to move their data from one organisation to another, and to object to their data being used at all.

The UK GDPR is relevant to online safety since it impacts on the way in which personal information should be secured on school networks, computers, and storage devices; and the security required for accessing, in order to prevent unauthorised access and dissemination of personal material.

Staff need to ensure that:

- Care is taken to ensure the safety and security of personal data regarding all of the school population and external stakeholders, particularly, but not exclusively: pupils, parents/carers, staff, and external agencies
- Personal and sensitive information should only be sent by email when on a secure network
- Personal data should only be stored on secure devices. In other words, only computers, servers, file-servers, cloud space, or devices which require a username and password to access the information
- Secure accounts need to be logged off after use to prevent unauthorised access
- Personal emails should not be used for school business

Data protection and protected characteristics

Care must be taken with data relating to protected characteristics:

- Information about pupils' gender identity, sexual orientation, or other protected characteristics must be handled with extreme sensitivity
- Pupils' chosen names and pronouns must be respected in digital systems
- Privacy settings must protect pupils exploring their identity
- Outing of pupils' protected characteristics without consent is a serious breach
- Data relating to protected characteristics should only be shared on a need-to-know basis and in accordance with safeguarding requirements
- Monitoring of online activity must be proportionate and must not target pupils based on protected characteristics

---

10. Monitoring

The E-Safety policy and Acceptable Use Policy are reviewed every 3 years. Additionally, the policy will be reviewed promptly upon:

- Serious and/or frequent breaches of the acceptable Internet use policy or incidents in the light of online safety incidents
- New guidance by government / LA / safeguarding authorities
- Significant changes in technology as used by the school or pupils in the wider community
- Online safety incidents in the community or local schools which might impact on the school community
- Advice from the Police and/or the Shropshire Safeguarding Partnership
- Changes to equality legislation or guidance

In line with Ofsted recommendations, it is useful to consult with pupils over the policy and where appropriate, to ask for their opinion on keeping themselves safe when using the Internet. The school will ensure that pupils with protected characteristics are included in consultation.

Equality monitoring

The school will monitor online safety incidents by protected characteristics, including:

- Recording protected characteristics in incident reports (with appropriate data protection)
- Analysing patterns of incidents by protected characteristic to identify trends
- Monitoring whether certain groups are disproportionately affected by online harms
- Evaluating whether responses are equitable across all groups
- Identifying any discriminatory patterns in filtering or monitoring

Annual reporting to governors will include:

- Patterns of online safety incidents
- Analysis by protected characteristics
- Actions taken to address disparities
- Effectiveness of equality training
- Compliance with the Public Sector Equality Duty
- Review of filtering and monitoring for equality impact

Accessibility of the policy

This policy is available in accessible formats including:

- Easy read versions
- Large print
- Audio format
- Translation into other languages upon request

---

11. Appendices

Appendix A: Acceptable Use Policy Agreement

This document describes the Acceptable Use Policy for any adult working with young people. The policy aims to ensure that any digital communications technology is used without creating unnecessary risk to users whilst supporting learning.

I agree that I will:

- Only use, move, and share personal data securely, with particular care for data relating to protected characteristics
- Respect the school network security
- Implement the school's policy on the use of technology and digital literacy including the skills of knowledge location, retrieval and evaluation, the recognition of bias, unreliability, and validity of sources
- Respect the copyright and intellectual property rights of others
- Only use approved email accounts
- Only use pupil images or work when approved by parents/registered care managers/social workers and in a way that will not enable individual pupils to be identified on a public facing site
- Only give permission to pupils to communicate online with trusted users
- Use the ICT facilities sensibly, professionally, lawfully, consistent with my duties and with respect for pupils and colleagues
- Respect all protected characteristics in my online communications and behaviour
- Challenge discrimination, hate speech, and offensive content online
- Promote equality and celebrate diversity in digital spaces

- Not use or share my personal (home) accounts/data (e.g., Facebook, email, eBay etc.) with pupils
- Set strong passwords which I will not share and will change regularly (a strong password is one which uses a combination of letters, numbers, and other permitted signs)
- Report unsuitable content and/or ICT misuse to the named E-Safety officer/DSL
- Report incidents of online discrimination, hate speech, or harassment
- Promote any supplied E-safety guidance appropriately

I know that anything I share online, store digitally or use on a digital device may be monitored.

I know that once I share anything online it is completely out of my control and may be used by others in a way that I did not intend.

I agree that I will not:

Visit internet sites, make, post, download, upload or pass on, material, remarks, proposals, or comments that contain or relate to:

- Inappropriate images
- Promoting discrimination of any kind, including but not limited to discrimination based on:
    - Race or ethnicity
    - Religion or belief
    - Sex or gender
    - Gender identity or gender reassignment
    - Sexual orientation
    - Disability
    - Pregnancy and maternity
    - Age
- Promoting violence or bullying
- Promoting racial, religious, homophobic, biphobic, transphobic, or any other form of hatred
- Promoting illegal acts

- Breach any Local Authority/school policies, e.g., gambling
- Do anything which exposes others to danger
- Post any other information which may be offensive to others
- Forward chain letters
- Breach copyright law
- Use personal digital recording equipment including cameras, phones, or other devices for taking/transferring images of pupils or staff without permission
- Store images or other files off site without permission from the Headteacher or their delegated representative

I understand my responsibilities under the Equality Act 2010 to:

- Eliminate discrimination, harassment, and victimisation in online spaces
- Advance equality of opportunity in digital learning
- Foster good relations between people with different protected characteristics

I will ensure that any private social networking sites, blogs, etc. that I create or actively contribute to, do not compromise my professional role **or contain discriminatory content**. I understand that data protection policy requires me to keep any information I see regarding staff or pupils, which is held within the school's management information system private, secure, and confidential. The only exceptions are when there is a safeguarding issue, or I am required by law to disclose such information to an appropriate authority.

I accept that my use of the school ICT facilities and any digital device used in connection with the school or school members may be monitored and the outcomes of the monitoring may be used.

Signed: _____ **Date:** _____

Name: _____

Appendix B: Flowchart for responding to E-Safety incidents

[Note: The flowchart image from the original document would be included here. The flowchart should be updated to include specific pathways for incidents involving protected characteristics, such as hate speech, discrimination, and outing.]

Additional considerations for incidents involving protected characteristics:

1. **Immediate response:**

- Ensure pupil safety
- Preserve evidence
- Protect privacy (especially important for LGBTQ+ pupils)

2. **Assessment:**
    - Is this a hate crime or hate incident?
    - Does it involve outing of protected characteristics?
    - Are there intersectional factors?
3. **Reporting:**
    - DSL/DDSL
    - Police (if hate crime)
    - Specialist organizations (e.g., LGBTQ+ support, anti-racism organizations)
    - Parents/carers (with consideration for confidentiality)
4. **Support:**
    - Victim support (including access to specialist services)
    - Restorative approaches where appropriate
    - Education for perpetrator(s)
5. **Recording:**
    - Record protected characteristics involved
    - Document actions taken
    - Include in equality monitoring

Appendix C: Useful links to external organisations

General online safety:

- CEOP (Child Exploitation and Online Protection Centre): www.ceop.police.uk
- Childline: www.childline.org.uk
- Childnet: www.childnet.com
- Internet Watch Foundation (IWF): www.iwf.org.uk
- Think U Know website: www.thinkuknow.co.uk

- UK Safer Internet Centre: www.saferinternet.org.uk

LGBTQ+ support:

- Mermaids (transgender youth support): www.mermaidsuk.org.uk
- Stonewall: www.stonewall.org.uk
- LGBT Foundation: www.lgbt.foundation
- MindOut (LGBTQ+ mental health): www.mindout.org.uk
- The Proud Trust: www.theproudtrust.org

Anti-racism and diversity:

- Show Racism the Red Card: www.theredcard.org
- Kick It Out: www.kickitout.org
- Tell MAMA (Measuring Anti-Muslim Attacks): www.tellmamauk.org
- Community Security Trust (antisemitism): www.cst.org.uk

Disability support:

- Scope: www.scope.org.uk
- Mencap: www.mencap.org.uk
- National Autistic Society: www.autism.org.uk

Reporting hate crime:

- True Vision (report hate crime): www.report-it.org.uk
- Police: In an emergency (a life is in danger or a crime in progress) dial 999. For other non-urgent enquiries contact local Police on 101

Safeguarding:

- Shropshire Safeguarding Partnership: safeguardingshropshireschildren.org.uk
- NSPCC: www.nspcc.org.uk

Appendix D: E-Safety Audit

This self-audit should be completed by the member of the Senior Leadership Team (SLT) responsible for E-Safety policy. Staff who could contribute to the audit include the Designated Safeguarding Lead, SENDCo and Headteacher.

Question	Y/N
Has the school an E-Safety policy that complies with DfE guidance?	
Date of latest update:	
Date of future review:	
The school E-Safety policy was agreed by the governors on:	
The policy is available for staff to access at:	
The policy is available for parents/carers to access at:	
Is the policy available in accessible formats?	
The responsible member of the Senior Leadership Team is:	
The Designated Safeguarding Lead is:	
The Deputy Designated Safeguarding Leads are:	
The E-Safety Coordinator is:	
Were all stakeholders (e.g., pupils, staff, parents/carers) consulted when updating the school E-Safety policy?	
Were pupils with protected characteristics specifically consulted?	
Has up-to-date E-Safety training been provided for all members of school staff?	
Does E-Safety training include equality and diversity?	
Do all staff sign an Acceptable Use Policy on appointment?	

Question	Y/N
Are all staff made aware of the school's expectation around safe and professional online behaviour?	
Are staff aware of their responsibilities under the Equality Act 2010?	
Is there a clear procedure for staff, pupils, and parents/carers to follow when responding to or reporting an online safety incident or concern?	
Are reporting mechanisms accessible to all pupils, including those with disabilities?	
Does the school have access to online safety materials from CEOP, Childnet etc.?	
Does the school have access to specialist resources on equality and online safety?	
Is online safety training provided for all pupils (appropriate to age and ability)?	
Is online safety teaching accessible to pupils with learning disabilities?	
Does online safety teaching address discrimination across all protected characteristics?	
Are online safety rules displayed in all classrooms where computers are used and expressed in a form that is accessible to all pupils?	
Do parents/carers or pupils sign an Acceptable Use Policy?	
Are staff, pupils, parents/carers, and visitors aware that internet use is monitored?	
Has an ICT security audit been initiated by the Senior Leadership Team?	

Question	Y/N
Has an equality impact assessment of filtering been conducted?	
Is personal data collected, stored, and used according to the principles of UK GDPR?	
Is particular care taken with data relating to protected characteristics?	
Is internet access provided by an approved educational internet service provider which complies with DfE requirements?	
Has the school filtering been designed to reflect educational objectives and been approved by the Senior Leadership Team?	
Does filtering block hate sites while not blocking legitimate content related to protected characteristics?	
Are members of staff with responsibility for managing filtering and network access adequately supervised by a member of the Senior Leadership Team?	
Does the school log and record all online safety incidents, including any action taken?	
Does the school record protected characteristics in incident reports and analyse patterns?	
Does the school report annually to governors on equality dimensions of online safety?	
Are the Governing Body and Senior Leadership Team monitoring and evaluating the school E-Safety policy and ethos on a regular basis?	

Appendix E: Equality monitoring template

Online Safety Incident Report - Equality Monitoring

Date of incident: _____

Type of incident: (tick all that apply)

- Cyberbullying
- Hate speech/discrimination
- Sexual harassment
- Sharing of inappropriate images
- Grooming
- Other (specify): _____

Protected characteristics involved: (tick all that apply)

- Age
- Disability
- Gender reassignment
- Pregnancy and maternity
- Race/ethnicity
- Religion or belief
- Sex/gender
- Sexual orientation
- None/not applicable
- Unknown

Specific type of discrimination: (if applicable)

- Racist
- Homophobic
- Biphobic
- Transphobic
- Sexist/misogynistic
- Ableist
- Religious discrimination
- Other: _____

Was this a hate crime/hate incident?

- Yes - reported to police
- Potential - under review
- No

Action taken:

- Reported to DSL/DDSL
- Reported to police
- Reported to social media platform
- Victim support provided
- Perpetrator education/consequences
- Specialist agency involved (specify): _____
- Restorative approach used
- Other: _____

Outcome:

Completed by: _____ **Date:** _____

Monitoring

	Signature	Date
Policy Reviewed By: Domoni Supple	D.Supple	22/06/26
Next Review Date:		01/06/29
Interim Review Comments:	Updated to include comprehensive equality provisions across all protected characteristics. Updated DSL/DDSL roles. Enhanced training	

	Signature	Date
	requirements. Added equality monitoring framework.	
Policy Reviewed By:		
Next Review Date:		
Interim Review Comments:		
Policy Reviewed By:		
Next Review Date:		
Interim Review Comments:		