Online Safety Policy

Title	Online Safety Policy
Author/Owner	Trust Board
Status	Final
Ratified Date	September 2026
Ratified by	Trust Board
Staff Consultation Date	5 October 2026 (via iAMCompliant)
Review Cycle	Annual
Review Date	September 2027
Security Classification	OFFICIAL

Contents

1	Aims	3
2	Application	3
3	Definitions	3
4	Responsibility for this Policy	4
5	Filtering and Monitoring	10
6	Access to the DET/School Technology	11
7	Use of Personal Mobile Electronic Devices and Smart Technology	12
8	Procedures for Dealing with Incidents of Misuse	13
9	Education	15
10	Training	17
11	Cybercrime	20
12	Risk Assessment	21
13	Record Keeping	21
14	Publication, Availability and Feedback	22

Appendix

Appendix 1	Regulatory Framework	23
Appendix 2	Other Relevant Policies	25

Updates since last version:

Throughout	Updated the Chief Financial and Operations Officer / CFOO to Chief Executive Officer/CEO as a point of contact to escalate concerns to as well as the Trust Director of Education Removed references to Director of HR Removed references to Executive Headteacher/EHT Removed References to Chief Financial and Operations Officer / CFOO

1 Aims

1.1 This is the Online Safety Policy of Discovery Educational Trust (DET) for the pupils of all DET Schools.

1.2 The aims of this Policy are as follows:

1.2.1 to protect DET and all School communities from potentially illegal, inappropriate and harmful content or contact;

1.2.2 to educate the entire DET/School community about access to and use of technology (including generative Artificial Intelligence (AI);

1.2.3 to establish effective mechanisms to identify, intervene in and escalate concerns where appropriate; and

1.2.4 to help to promote a whole-Trust and whole-School culture of openness, safety, equality and protection.

1.3 This Policy forms part of the DET whole-Trust and School approach to promoting child safeguarding and wellbeing, which involves everyone at DET/its Schools and seeks to ensure that the best interests of pupils are at the forefront of all decisions, systems, processes and policies.

1.4 Online safety informs many of DET/School policies and procedures (including the DET Safeguarding and Child Protection Policy and local School procedures). Careful consideration has been given to ensure that it is also reflected in all School curricula, teacher training and any parental engagement, as well as the role and responsibility of the Schools' Designated Safeguarding Leads (**DSLs**) (and any deputies).

2 Application

2.1 This Policy applies to the whole of all DET Schools, including the Early Years Foundation Stage (EYFS) and Sixth Form.

2.2 This Policy applies to all members of the DET/School community, including staff and volunteers, pupils, Parents and visitors, who have access to DET/School technology (including generative AI) whether on or off DET/School premises, or otherwise use technology (including generative AI) in a way which affects the welfare of other pupils or any member of the DET/School community or where the culture or reputation of DET/its Schools is put at risk.

3 Definitions

3.1 Where the following words or phrases are used in this Policy:

3.1.1 The Online Safety Policy is referred to as **this Policy;**

3.1.2 **Parent** or **Parents** means the natural or adoptive Parents of the pupil (irrespective of whether they are or have ever been married, with whom the pupil lives, or whether they have contact with the pupil) as well as any person, who is not the natural or adoptive Parent of the pupil, but who has care of, or Parental responsibility for, the pupil (e.g. foster carer/legal guardian);]

3.1.3 **School days** mean any day on which there is a school session to which attendance is required;

3.1.4 References to **DET/Trust** are references to Discovery Educational Trust.

3.1.5 References to staff includes all those who work for or on behalf of DET/its Schools, regardless of their employment status, including contractors, supply staff, volunteers, Members, Trustees and Local Governors, unless otherwise indicated.

3.1.6 Senior Leadership Team (**SLT**) comprises of the Headteacher (HT), Deputy Headteachers(s) (DHT), Assistant Headteacher(s) (AHT) and School Business Manager (SBM), if appropriate. The role of DSL is assumed by one of the SLT members.

3.1.7 In considering the scope of the DET/School online safety strategy, DET and its Schools will take a wide and purposive approach to considering what falls within the meaning of technology (including generative AI), networks and devices used for viewing or exchanging information (collectively referred to in this Policy as **technology**).

4 Responsibility for this Policy

4.1 The Trust (DET) has overall responsibility for all matters, which are the subject of this Policy.

4.2 DET will comply with its duties under the Children and Families Act 2014, the Equality Act 2010 and the specific requirement under section 149 of the Equality Act 2010 to meet the Public Sector Equality Duty. This means that, in carrying out its functions, the Trust is required to have due regard to the need to:

4.2.1 eliminate discrimination and other conduct that is prohibited by the Act;

4.2.2 advance equality of opportunity between people who share a protected characteristic and people who do not share it; and

4.2.3 foster good relations across all characteristics between people who share a protected characteristic and people who do not share it.

4.3 **SLT members will:**

4.3.1 The HT has overall executive responsibility for the safety and welfare of members of the School community. This includes a specific responsibility to ensure that the School has an effective filtering policy in place and that it is applied and updated on a regular basis.

4.3.2 The DSL is a member of each School's SLT with lead responsibility for safeguarding and child protection, including online safety, and understanding the filtering and monitoring systems in place in the School.

4.3.3 The responsibility of the DSL includes:

(a) managing safeguarding incidents involving the use of technology in the same way as other safeguarding matters, in accordance with the DET Safeguarding and Child Protection Policy and local School procedures;

(b) working with the SLT Digital Lead (refer below) to ensure that all staff are appropriately trained and aware of the procedures that need to be followed in the event of an online safety incident and the need to immediately report those incidents;

(c) working with the School's Network Manager and SLT Digital Lead (refer below) in monitoring technology uses and practices across the School and assessing whether any improvements can be made to ensure the online safety and wellbeing of pupils. 360 degree safe: the online safety self-review tool will be used to assist with this process;

(d) overseeing and acting on: filtering and monitoring reports, safeguarding concerns and checks to filtering and monitoring systems;

(e) regularly monitoring the technology incident log maintained by the Network Managers and working with the SLT Digital Lead (refer below) to assess whether changes need to be made to the digital technology strategy and staff and pupil training;

(f) regularly updating other members of the School's SLT and the DET TB on the operation of the School's safeguarding arrangements, including online safety practices;

(g) providing online safety training and advice for Local Governors, staff, Parents and pupils, including on online harms and how to identify illegal, harmful or inappropriate content, including content created or accessed through the use of generative AI;

(h) promoting an awareness of and commitment to online safety education/awareness raising across the School and beyond.

4.4 **SLT Digital Lead**

4.4.1 The SLT Digital Lead is a member of the SLT with lead responsibility for digital technology. They act as a link between technical staff, the SLT, curriculum leads, GDPR Leads, the DSL, the School Business Manager, the School's Network Manager and the Trust's Director of IT and Estates.

4.4.2 The SLT Digital Lead should have strategic oversight of all digital technology. They will create and manage the digital technology strategy led by the needs of staff and pupils.

4.4.3 The SLT Digital Lead will be accountable for:

(a) the delivery of the digital technology strategy based on teaching and learning outcomes and organisational needs;

(b) encouraging and supporting the use of digital technology across the School;

(c) reviewing the effectiveness of IT support to inform decision making and taking action, when necessary;

(d) identifying and acting on digital technology training needs for staff and pupils.

4.4.4 The SLT Digital Lead will also be responsible for:

(a) reviewing registers relating to hardware and systems to ensure that they are accurate and complete;

(b) reviewing measures in place on the School's use of generative AI and measures taken to combat cybercrime;

(c) proactively identifying any potential compromises to safeguarding or risk of a cyber-attack to ensure compliance with the cyber security standards;

(d) ensuring that digital technology is included within insurance arrangements and disaster recovery and business continuity plans;

(e) overseeing and acting on: arrangements for information and cyber security and action taken to meet the cyber security standards to protect the School from cyber-attacks and to improve cyber resilience.

4.5 **Trust Director of IT and Estates**

4.5.1 The Trust Director of IT and Estates, together with their team, is responsible for the effective operation of the DET/Schools' filtering system in order that pupils and staff are unable to access any material that poses a safeguarding risk, including terrorist and extremist material, while using the Trust/School network.

4.5.2 The Trust Director of IT and Estates is responsible for ensuring that:

(a) the DET/School technology infrastructure is secure and, so far as is possible, is not open to misuse or malicious or cyber-attack;

(b) the user may only use the DET/School technology if they are properly authenticated and authorised;

(c) filtering and monitoring systems are maintained, providing filtering and monitoring reports and completing actions following concerns or checks to systems;

(d) the risks of pupils and staff circumventing the safeguards put in place by the Trust/School are minimised;

(e) the use of the Trust/School technology is regularly monitored to ensure compliance with this Policy and that any misuse or attempted misuse can be identified and reported to the appropriate person for investigation; and

(f) monitoring software and systems are kept up to date to allow the IT team to monitor the use of email and the internet over the DET/School network and maintain logs of such usage.

4.5.3 To ensure the highest standards of online safety and compliance with safeguarding obligations, the Trust has implemented robust technical provisions for filtering, monitoring, and alerting. It utilises an industry-leading cloud-based solution to actively block access to inappropriate or harmful online content in real time. These filtering systems apply age-appropriate rules across all devices used within the School network.

In addition to filtering, the solution provides monitoring and reporting features, enabling continuous oversight of online activity. Alerts are automatically generated and escalated for any content or behaviour flagged as a potential safeguarding risk. These alerts are reviewed promptly by the DSL or DDSL, ensuring that timely and appropriate interventions can be made in accordance with the DET Safeguarding and Child Protection Policy, local School procedures and any statutory guidance, such as KCSiE.

4.5.4 The Trust Director of IT and Estates will report regularly to Trustees on the operation of the DET/Schools' technology. If the Trust Director of IT and Estates has concerns about the functionality, effectiveness, appropriateness or use of technology within the DET/its Schools, including of the monitoring and filtering systems in place, they will escalate those concerns promptly to the Trust Director of Education – Pastoral and the Chief Executive Officer (CEO).

4.5.5 The Trust Director of IT and Estates is responsible for maintaining the technology incident log (a central record of all serious incidents involving the use of technology) and bringing any matters of a safeguarding concern to the attention of the Director of Education – Pastoral, in accordance with the DET Safeguarding and Child Protection Policy and local School procedures.

4.6 **All members of staff**

4.6.1 All staff have a responsibility to act as good role models in their use of technology and to share their knowledge of the DET/School policies and of safe practice with pupils.

4.6.2 Staff are expected to adhere, so far as applicable, to each of the policies referenced in this Policy.

4.6.3 Training for staff includes online safety which, amongst other things, includes an understanding of filtering and monitoring provisions in place, how to manage them effectively, the use of generative AI and the risks associated with this, how to escalate concerns when identified and any particular expectations or responsibilities in relation to filtering and monitoring.

4.6.4 All staff are aware that technology can play a significant part in many safeguarding and wellbeing issues and that pupils are at risk of abuse online as well as face-to-face. Staff are also aware that, sometimes, such abuse will take place concurrently online and during a pupil's daily life.

4.6.5 Staff are expected to be alert to the possibility of pupils abusing their peers online and to understand that this can occur both inside and outside of School. Examples of such abuse can include:

(a) the sending of abusive, harassing and misogynistic/misandrist messages;

(b) the consensual and non-consensual sharing of indecent images and videos (especially around group chats), which is sometimes known as sexting or youth-produced sexual imagery. This includes the sharing of digitally manipulated or AI-generated images;

(c) the sharing of abusive images and pornography to those who do not wish to receive such content;

(d) cyberbullying.

4.6.6 Staff are also aware that many other forms of abuse may include an online element. For instance, there may be an online element which:

(a) facilitates, threatens and/or encourages physical abuse;

(b) facilitates, threatens and/or encourages sexual violence; or

(c) is used as part of initiation/hazing-type violence and rituals.

4.6.7 It is important that staff recognise the indicators and signs of child-on-child abuse, including where such abuse takes place online, and that they know how to identify it and respond to reports. Staff must also understand that, even if there are no reports of child-on-child abuse at the School, whether online or otherwise, it does not mean that it is not happening; it may simply be the case that it is not being reported.

4.6.8 It is important that staff challenge inappropriate behaviours between peers and do not downplay certain behaviours, including sexual violence and sexual harassment, as "*just banter*", "*just having a laugh*", "*part of growing up*", "*boys being boys*" or *"girls being girls"* as doing so can result in a culture of unacceptable behaviours, an unsafe environment for children and, in a worst-case scenario, a culture that normalises abuse.

4.6.9 DET and its Schools have a **zero-tolerance approach** towards child-on-child abuse (including in relation to sexual violence and sexual harassment) and such behaviour is never acceptable and will not be tolerated. DET and its Schools will treat any such incidences as a breach of discipline and will deal with them under the School's Behaviour Policy and also as a safeguarding matter under the DET Safeguarding and Child Protection Policy and local School procedures.

4.6.10 Staff have a responsibility to report any concerns about a pupil's welfare and safety to the DSL and, in accordance with this Policy and the DET Safeguarding and Child Protection Policy and local School procedures. If staff have any concerns regarding child-on-child abuse or if they are unsure as to how to proceed in relation to a particular incident, they should **always speak to the DSL**.

4.7 DET will be responsible for providing suitable training to all staff on all matters related to this Policy. This includes:

4.7.1 DET has overall responsibility for safeguarding arrangements within all Trust Schools, including the approach to online safety and the use of technology within all Schools.

4.7.2 The Safeguarding Link Trustee is the senior board-level lead with leadership responsibility for the Trust's and the Schools' safeguarding arrangements, including the School online safety procedures, on behalf of DET.

4.8 The level and frequency of training depends on the role of the individual member of staff. All DET Schools maintain written records of all staff training.

4.9 In order to achieve full and effective implementation of this Policy, DET has allocated the following tasks:

Task	Allocated to	When / frequency of review
Keeping the Policy up-to-date and compliant with the law and best practice	Director of Education – Pastoral; and Director of HR, Operations & Governance	As required, and, at least, termly
Monitoring the implementation of the Policy (including the record of incidents involving the use of technology and the logs of internet activity and sites visited), relevant risk assessments and any action taken in response and evaluating effectiveness.	DSL or DDSL	As required, and, at least, termly
Online safety	DSL	As required and, at least, annually
Assessing the Trust/School approach to filtering and monitoring and assessing this in light of new or emerging risks and technologies.	SLT, DSL, Network Manager, IT service provider and Safeguarding Link Governor	As required, and, at least, annually
Reviewing digital technology strategy	Director of IT and Estates and IT team members	As required, and, at least, annually
Taking appropriate action to meet the Cyber security standards for schools and colleges[1]	Director of IT and Estates and Network Managers	As required, and, at least, annually
Seeking input from interested groups (such as pupils, staff, Parents) to consider improvements to the school's processes under the Policy.	DSL or DDSL	As required, ideally, termly
Maintaining up-to-date records of all information created in relation to the Policy and its	School GDPR Lead	As required, and, at least, termly

[1] The Cyber security standards for schools and colleges were developed to help schools improve their resilience against cyber-attacks. Broader guidance on cyber security including considerations for governors and trustees can be found at National Cyber Security Centre – NCSC.

Task	Allocated to	When / frequency of review
implementation as required by the UK GDPR.		
Formal annual review.	DET Trust Board (TB)	Annually
Overall responsibility for content and implementation.	DET	As a minimum annually

4.10 **Parents**

4.10.1 The role of Parents in ensuring that pupils understand how to stay safe when using technology is crucial. DET and its Schools expect Parents to promote safe practice when using technology and to:

(a) support DET/its Schools to implement this Policy and report any concerns in line with the DET/School policies and procedures;

(b) talk to their child to understand the ways in which they are using the internet, social media and their mobile devices, and promote responsible behaviour;

(c) encourage their child to speak to someone if they are being bullied or otherwise are concerned about their own safety or that of another pupil or need support; and

(d) support the School's policy on prohibiting the use of mobile phones.

4.10.2 If Parents have any concerns or require any information about online safety, they should contact the relevant School's DSL.

5 Filtering and Monitoring

5.1 Whilst considering their responsibility to safeguard and promote the welfare of pupils and provide them with a safe environment in which to learn, DET will do all it reasonably can to limit pupil's exposure to risks from the DET/School IT system. As part of this process, DET and its Schools have appropriate filtering and monitoring systems in place and regularly review their effectiveness.

5.2 DET and its Schools have regard to Government filtering and monitoring standards, which require that DET/its Schools:

5.2.1 identify and assign roles and responsibilities to manage filtering and monitoring systems;

5.2.2 have effective monitoring strategies in place that meet their safeguarding needs;

5.2.3 review filtering and monitoring provision and its effectiveness, at least, annually; and

5.2.4 block harmful and inappropriate content without unreasonably impacting teaching and learning.

5.3 DET and its Schools will assess their approach to filtering and monitoring to reflect the risks that they face and will continue to assess this in light of new or emerging risks and technologies[2].

5.4 DET/its Schools manage access and restrictions to content across its systems for all users, including guest accounts. Logs/alerts are regularly reviewed and acted upon.

5.5 DET/its Schools have provided enhanced/differentiated user-level filtering (allowing different filtering levels for different abilities/ages/stages and different groups of users: staff/learners, etc.). Younger learners use child friendly/age-appropriate search engines e.g. SWGfL, Swiggle.

5.6 DET/its Schools understand the extent to which content is dynamically analysed where it is streamed in real-time (including content created by users or through generative AI) to the user and blocked.

5.7 Access to content through non-browser services, for example, apps and other mobile technologies, is managed in ways that are consistent with this Policy.

5.8 DET/its Schools have monitoring systems in place to protect them, their systems and users. All network use across all its devices and services is monitored. Logs/alerts are regularly reviewed and acted upon.

5.9 DET/its Schools use a number of monitoring strategies to minimise safeguarding risks on internet-connected devices, including:

5.9.1 physical monitoring by staff watching screens of users;

5.9.2 live supervision by staff on a console with device management software;

5.9.3 network monitoring using log files of internet traffic and web access; and

5.10 individual device monitoring through software or third-party services.

6 Access to the DET/School Technology

6.1 DET/its Schools provide internet, intranet and social media access and an email system to pupils and staff as well as other technology. Pupils and staff must comply with the respective acceptable use policy when using DET/School technology. All such use is monitored by the IT team.

6.2 Pupils and staff require individual user names and passwords to access the DET/School internet, intranet and social media sites and email system, which must not be disclosed to any other person. Any pupil or member of staff, who has a problem with their user names or passwords, must report it to the relevant IT Support Team immediately.

6.3 No laptop or other mobile electronic device may be connected to the DET/School network without the consent of the IT Support Team. The use of any device connected to the DET/School network will be logged and monitored by the IT Support Team. See also 6.5 below and the DET Information Governance suite of policies, which apply across DET and its Schools (including remote working and bring your own device to work).

[2] See Plan technology for your school (HM Government, September 2024) which includes a self-assessment tool to assist schools in meeting the filtering and monitoring standards

6.4 Each Trust School has a separate wireless network connection available for use by visitors to the School. A password, which is changed on a regular basis, must be obtained from a member of staff in order to use the wireless network. Use of this service will be logged and monitored by the IT Support Team.

6.5 **Inappropriate Material**

6.5.1 DET/its Schools recognise the importance of ensuring that all pupils are safeguarded from potentially harmful and inappropriate material online.

6.5.2 Online safety is a key element of many DET/School policies and procedures and an important part of the role and responsibilities of the SLT Digital Lead. The term "online safety" encapsulates a wide range of ever-evolving issues, but these can be classified into four main areas of risk:

(a) **Content**: being exposed to illegal, inappropriate or harmful content including, for example, pornography, fake news, racism, misogyny, misandry, self-harm, suicide, anti-Semitism, radicalisation and extremism, misinformation, disinformation (including fake news) and conspiracy theories;

(b) **Contact**: being subjected to harmful online interaction with other users, for example, peer-to-peer/child-on-child pressure, commercial advertising and adults posing as children or young adults with the intention to groom and/or exploit them for sexual, criminal, financial or other purposes;

(c) **Conduct**: online behaviour that increases the likelihood of, or causes, harm, for example, making, sending and receiving explicit images (such as the consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and

(d) **Commerce**: risks, such as online gambling, inappropriate advertising, phishing and/or financial scams. If pupils or staff are at risk, it should be reported to the Anti-Phishing Working Group[3].

7 Use of Personal Mobile Electronic Devices and Smart Technology

7.1.1 The School rules about the use of personal mobile electronic devices or other smart technology, including access to open/non-School networks and the use of generative AI tools, are clearly and regularly communicated to all staff and pupils and are detailed in the DET Generative AI Policy, the Acceptable Personal Use of Resources and Assets Policy and the acceptable use agreements signed by pupils.

7.1.2 Each School will consider whether adaptations and reasonable adjustments to this policy need to be made for individual pupils, for example, to manage medical conditions or for safeguarding reasons. These will be considered on a case-by-case basis and permission to do so must be sought and provided in advance.

7.1.3 All Schools do all that they reasonably can to limit children's exposure to the risks identified above through the use of the DET/School IT systems, including robust activity logging procedures to monitor content and usage within each School to identify patterns of misuse or suspected misuse.

7.1.4 DET and its schools have effective filtering and monitoring systems in place to safeguard pupils when accessing the internet—including email and social media—whilst using the School's Wi-Fi, on either personal or School-issued devices that are connected to the DET or School network.

The effectiveness of these systems is regularly reviewed to ensure ongoing protection. Any devices that are not managed by DET/its Schools should be connected to a separate virtual network to maintain network security and safeguarding standards.

7.1.5 Mobile devices and smart technology, equipped with a mobile data subscription, can, however, provide pupils with unlimited and unrestricted access to the internet. DET/its Schools are alert to the risks that such access presents, including the risk of pupils sexually harassing, bullying or controlling their peers using their mobile or other smart technology; or sharing indecent images consensually or non-consensually (often via large group chats); or viewing and/or sharing pornography and other illegal, inappropriate or harmful content (including content created by generative AI tools in real-time). DET/its Schools have adopted a policy of prohibiting all pupils from using personal mobile devices whilst on the School site as a mechanism to manage such risks.

7.1.6 The use of personal mobile electronic devices by staff is covered in the DET Staff Code of Conduct and in the DET Acceptable Personal Use of Resources and Assets Policy.

8 Procedures for Dealing with Incidents of Misuse

8.1 Staff, pupils and Parents are required to report incidents of misuse or suspected misuse to DET/its Schools in accordance with this Policy, the DET Safeguarding and Child Protection Policy and disciplinary policies and procedures.

8.2 DET and its Schools recognise the importance of acknowledging, understanding and not downplaying behaviours, which may be related to abuse, and has appropriate systems in place to ensure that pupils can report any incidents of abuse, whether or not they include an online element, confidently and safe in the knowledge that their concerns will be treated seriously. Staff should, however, be careful not to promise that a concern will be dealt with confidentially at an early stage as information may need to shared further, for example, with the DSL to discuss next steps.

8.3 Misuse by Pupils

8.3.1 **Anyone,** who has **any** concern about the misuse of technology by pupils, should report it immediately to the appropriate member of staff (referred to in the table below) so that it can be dealt with in accordance with the School Behaviour Policy, including the School Anti-Bullying Policy where there is an allegation of cyberbullying.

Type of misuses	Relevant policy	Reporting channel
Bullying	Anti-bullying	As advised in the School Anti-Bullying Policy. Note: any incidents, which give rise to safeguarding concerns must be referred to the DSL. All incidents must be reported on CPOMS.
Sharing nudes and semi-nude images (sexting/youth-produced sexual imagery).	Safeguarding and Child Protection Policy and local School procedures.	All incidents must be referred to the DSL, who has overall responsibility for online safety matters. All incidents must be reported on CPOMS.
Sexual violence and sexual harassment (whether during or outside of School).	Safeguarding and Child Protection Policy and local School procedures.	The DSL, who has overall responsibility for online safety matters. All incidents must be reported on CPOMS.
Harassment	Safeguarding and Child Protection Policy and local School procedures.	All incidents must be referred to the DSL, who has overall responsibility for online safety matters. All incidents must be reported on CPOMS.
Upskirting	Safeguarding and Child Protection Policy and local School procedures.	All incidents must be referred to the DSL, who has overall responsibility for online safety matters. All incidents must be reported on CPOMS.
Radicalisation	Safeguarding and Child Protection Policy and local School procedures.	All incidents must be referred to the DSL, who has overall responsibility for online safety matters. All incidents must be reported on CPOMS.
Any action resulting in disruption to digital technology systems in School.	Digital technology strategy	SLT Digital Lead Note: any incidents, which give rise to safeguarding concerns

		must be referred to the DSL and reported on CPOMS.
Other breach of acceptable use policy, including unauthorised use of personal mobile devices on School sites.	Staff Code of Conduct, Acceptable Personal Use of Resources and Assets Policy (for staff) and acceptable use agreements (for pupils).	All incidents must be referred to the DSL, who has overall responsibility for online safety matters. Note: any incidents, which give rise to safeguarding concerns must be referred to the DSL and reported on CPOMS.

8.3.2 **Anyone,** who has **an**y concern about the welfare and safety of a pupil must report it immediately in accordance with the DET Safeguarding and Child Protection Policy and local School procedures.

8.4 **Misuse by Staff**

8.4.1 If anyone has a safeguarding-related concern relating to staff misuse of technology, they must report it immediately in accordance with the DET Safeguarding and Child protection Policy, Appendix 5 - Raising Allegations and Low-Level Concerns.

8.4.2 Anyone, who has any other concern about the misuse of technology by staff, should report their concerns immediately in accordance with the DET Safeguarding and Child protection Policy, Appendix 5 - Raising Allegations and Low-Level Concerns.

8.5 **Misuse by any User**

8.5.1 **Anyone,** who has **any** concern about the misuse of technology by any other user, should report it immediately to the HT and the DSL (or DDSL).

8.5.2 DET/its Schools reserve the right to withdraw access to the DET/School network by any user at any time and to report suspected illegal activity to the police.

8.6 If DET/its Schools consider that any person is vulnerable to radicalisation, they will refer this to the Channel programme. This programme focuses on support at an early stage to people, who are identified as being vulnerable to being drawn into terrorism. Any person, who has a concern relating to extremism, may report it directly to the police.

9 Education

9.1 The teaching of online safety is integrated, aligned and considered as part of the whole-DET/School safeguarding approach and wider staff training and curriculum planning.

9.2 DET and its Schools ensure that children are taught how to keep themselves and others safe, including online, and the safe use of technology is, therefore, integral to each School's curriculum. Pupils are educated in an age-appropriate manner about the importance of safe and responsible use of technology, including the internet, social media and mobile electronic devices and on the use of generative AI tools (refer to each School's curriculum). Teaching is tailored to the specific needs and vulnerabilities of individual children, such as those, who are victims of abuse, children with special educational needs or disabilities (SEND).

9.3 The safe use of technology is a focus in all areas of the curriculum and teacher training, and key safety messages are reinforced as part of assemblies and tutorial/pastoral activities and teaching pupils:

9.3.1 about the risks associated with using the technology and how to protect themselves and their peers from potential risks;

9.3.2 about the importance of identifying, addressing and reporting inappropriate behaviour, whether on or offline, and the risks of downplaying such behaviour as, for example, "*banter*", "*just boys being boys*" or "just girls being girls";

9.3.3 to be critically aware of content they access online (including how to recognise illegal, inappropriate or harmful content) and guided to validate accuracy of information;

9.3.4 to be aware of and how to identify the risks posed by cybercrime;

9.3.5 how to recognise suspicious, manipulative, dishonest, bullying or extremist behaviour;

9.3.6 the definition of cyberbullying, its effects on the victim and how to treat each other's online identities with respect;

9.3.7 the consequences of negative online behaviour;

9.3.8 how to report cyberbullying and/or incidents that make pupils feel uncomfortable or under threat and how DET/its Schools will deal with those who behave badly; and

9.3.9 how to respond to harmful online challenges and hoaxes.

9.4 DET and its Schools recognise the crucial role they play in relation to preventative education and that this is most effective in the context of a whole-School approach that prepares pupils for a life in modern Britain and creates a culture of zero-tolerance for sexism, misogyny /misandry, homophobia, biphobia and sexual violence and sexual harassment.

9.5 Pupils are taught about the risks associated with all forms of abuse, including physical abuse and sexual violence and sexual harassment, which may include an online element. DET and its Schools have a zero-tolerance approach to sexual violence and sexual harassment and such behaviour is never acceptable and will not be tolerated. DET and its Schools will treat any such incidences as a breach of discipline and will deal with them under the Schools' Behaviour Policies, and also as a safeguarding matter under the DET Safeguarding and Child Protection Policy and local School procedures.

9.6 Those parts of the curriculum, which deal with the safe use of technology are reviewed on a regular basis to ensure their relevance.

9.7 All DET Schools regularly remind pupils (and Parents) on the rules that govern the use of technology, including internet, email, social media and personal mobile electronic devices, helping pupils to protect themselves and others when using technology.

9.8 DET and its Schools recognise that effective education needs to be tailored to the specific needs and vulnerabilities of individual pupils, including those who are victims of abuse, and those with special educational needs and disabilities, and this is considered when devising and implementing processes and procedures to ensure the online safety of all pupils. For more details on the DET/School approach, refer to the DET Safeguarding and Child Protection Policy and local School procedures as well as the PSHE and RSE curricula.

9.9 Technology is included in the educational programmes followed in the EYFS in the following ways:

9.9.1 children are guided to make sense of their physical world and their community through opportunities to explore, observe and find out about people, places, technology and the environment;

9.9.2 children are enabled to explore and play with a wide range of media and materials, and provided with opportunities and encouragement for sharing their thoughts, ideas and feelings through a variety of activities in art, music, movement, dance, role-play, and design and technology; and

9.9.3 children are guided to recognise that a range of technology is used in places such as homes and schools and encouraged to select and use technology for particular purposes.

9.10 Useful online safety resources for pupils:

9.10.1 CEOP Education ;

9.10.2 http://www.childnet.com/young-people;

9.10.3 EYFS only - https://childnet.com/resources/smartie-the-penguin;

9.10.4 EYFS only - https://www.childnet.com/resources/digiduck-stories;

9.10.5 https://www.saferinternet.org.uk/advice-centre/young-people;

9.10.6 https://mysafetynet.org.uk/;

9.10.7 https://www.ceop.police.uk/Safety-Centre/How-can-CEOP-help-me-YP/;

9.10.8 https://www.bbc.com/ownit.

10 Training

10.1 Trustees

10.1.1 All Trustees and Local Governors receive appropriate safeguarding and child protection (including online safety) training at induction. This training is regularly updated. This ensures that all Trustees are equipped with the knowledge to provide strategic challenge to test and assure themselves that the safeguarding policies and procedures of DET and its Schools are effective and that they support the delivery of a robust whole-School approach to safeguarding.

10.2 Staff

10.2.1 All Schools provide training on the safe use of technology to staff so that they are aware of how to protect pupils and themselves from the risks of using technology and to deal appropriately with incidents involving the use of technology when they occur. This includes being able to recognise the additional risks that children with SEN and disabilities (**SEND**) face online and that they are confident that they have the capability to support SEND children to stay safe online.

10.2.2 Induction training for new staff includes training on the DET/School online safety strategy including this Policy, the Staff Code of Conduct, the Generative AI Policy and the Acceptable Personal Use of Resources and Assets Policy. Training specifically addresses the DET/School filtering and monitoring provisions in place, including activity logging and reporting mechanisms, how to manage them effectively, how to escalate concerns, when identified, and any particular staff expectations or responsibilities, including on the use of approved generative AI tools for educational purposes.

10.2.3 Staff training is regularly updated and ongoing staff development training includes (but is not limited to) training on technology safety together with specific safeguarding issues, including sharing nude and semi-nude images and or videos, cyberbullying, radicalisation, dealing with harmful online challenges and online hoaxes and on the risks associated with generative AI tools and content created by them. This training may be in addition to the regular safeguarding and child protection (including online safety) updates, as required at induction and, at least, annually thereafter.

10.2.4 Where pupils wish to report a safeguarding concern, all staff are taught to reassure victims that they are being taken seriously and that they will be supported and kept safe. Staff are aware of the importance of their role in dealing with safeguarding and wellbeing issues, including those involving the use of technology, and understand that a victim should never be given the impression that they are creating a problem by reporting abuse, including sexual violence or sexual harassment, and nor should they ever be made to feel ashamed for making a report.

10.2.5 Where safeguarding incidents involve an online element, such as youth-produced sexual imagery, staff will not view or forward sexual imagery reported to them and will follow the DET Safeguarding and Child Protection Policy and local School procedures, which detail the process to follow for the sharing nudes and semi-nude images and videos. The DfE Searching, screening and confiscation: advice for schools (DfE, September 2022) should also be referenced. In certain cases, it may be more appropriate for staff to confiscate a pupil's devices to preserve any evidence and hand it to the police for inspection.

10.2.6 Staff are encouraged to adopt and maintain an attitude of "it could happen here" where safeguarding is concerned, including in relation to sexual violence and sexual harassment, and to address inappropriate behaviours (even where such behaviour appears relatively innocuous) as this can be an important means of intervention to help prevent problematic, abusive and/or violent behaviour in the future.

10.2.7 Staff are trained to recognise any illegal, inappropriate or harmful content, including content created through generative AI tools, and to look out for potential patterns of concerning, problematic or inappropriate behaviour and, where a pattern is identified, DET and its Schools will decide on an appropriate course of action to take. Consideration will also be given as to whether there are wider cultural issues within DET/School that facilitated the occurrence of the inappropriate behaviour and, where appropriate, extra teaching time and/or staff training will be delivered to minimise the risk of it happening again.

10.2.8 Staff also receive Data Protection training on induction and annually thereafter.

10.2.9 The frequency, level and focus of all such training will depend on individual roles and requirements and will be provided as part of the DET/School overarching approach to safeguarding.

10.2.10 Useful online safety resources for staff:

(a) https://www.saferinternet.org.uk/advice-centre/teachers-and-professionals;

(b) http://www.childnet.com/teachers-and-professionals;

(c) https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/;

(d) https://www.thinkuknow.co.uk/teachers/;

(e) http://educateagainsthate.com/;

(f) https://www.commonsense.org/education/;

(g) Cyberbullying: advice for head teachers and school staff (DfE, November 2014);

(h) Advice on the use of social media for online radicalisation (DfE and Home Office, July 2015);

(i) Sharing nudes and semi-nudes: advice for education settings working with children and young people (DfDCMS and UKCIS, March 2024);

(j) Using External Expertise to Enhance Online Safety Education (UKCIS, October 2022);

(k) Online safety in schools and colleges: questions from the governing board (UKCIS, June 2020);

(l) Education for a connected world framework (UKCIS, June 2020);

(m) https://www.lgfl.net/online-safety/resource-centre;

(n) Online Sexual Harassment: Understand, Prevent and Respond Guidance for Schools (Childnet, March 2019);

(o) Myth vs Reality: PSHE toolkit (Childnet, April 2019);

(p) SELMA Hack online hate toolkit (SWGFL, May 2019);

(q) Teaching online safety in schools (DfE, January 2023);

(r) Harmful online challenges and online hoaxes (DfE, February 2021);

(s) Professionals' online safety helpline: helpline@saferinternet.org.uk, 0344 381 4772;

(t) NSPCC helpline for anyone worried about a child - 0808 800 5000.

(u) Internet Watch Foundation - internet hotline for the public and IT professionals to report potentially criminal online content

10.2.11 The Essex Safeguarding Children Board and the Southend Safeguarding Partnership can provide guidance for Parents on radicalisation.

10.3 **Parents**

10.3.1 All DET Schools are in regular contact with Parents and use their communications to reinforce the importance of ensuring that children are safe online. All DET Schools aim to help Parents understand what systems are in place to filter and monitor their child's online use and ensures that Parents are aware of what their children are being asked to do online (including what sites they will be asked to access) and who from the School they will be interacting with online, if anyone.

10.3.2 Parents are encouraged to reinforce all communications around the School's acceptable use policy for pupils with their child to ensure that it is fully understood.

10.3.3 Parents have an important role in supporting the School's policy on prohibiting the use of mobile phones on the School site. Parents are encouraged to reinforce and discuss this policy with pupils, including the risks associated with mobile phone use and the benefits of a mobile phone-free environment.

10.3.4 Where Parents need to contact their child during the school day, they should be directed to the School Office, where staff should be aware of the School's policy on relaying messages and facilitating contact.

10.3.5 **Useful online safety resources for Parents**

(a) https://www.saferinternet.org.uk/advice-centre/parents-and-carers;

(b) http://www.childnet.com/parents-and-carers;

(c) https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/;

(d) https://www.thinkuknow.co.uk/parents/;

(e) http://parentzone.org.uk/;

(f) https://www.internetmatters.org/;

(g) https://www.commonsensemedia.org/;

(h) Advice for parents and carers on cyberbullying (DfE, November 2014);

(i) http://www.askaboutgames.com;

(j) https://www.ceop.police.uk/safety-centre;

(k) UK Chief Medical Officers' advice for parents and carers on children and young people's screen and social media use (February 2019);

(l) LGfL: parents - scare or prepare;

(m) Thinkuknow: what to do if there's a viral scare online.

11 Cybercrime

11.1 Cybercrime is criminal activity committed using computers and/or the internet. It is broadly categorised as either "cyber-enabled" (crimes that can happen offline, but are enabled at scale and at speed online) or "cyber dependent" (crimes that can be committed only by using a computer).

11.2 Cyber-dependent crimes include:

11.2.1 unauthorised access to computers (illegal "hacking"), for example, accessing a School's computer network to look for test paper answers or change grades awarded;

11.2.2 denial of service (**DoS** or **DDoS**) attacks or "booting", which are attempts to make a computer, network or website unavailable by overwhelming it with internet traffic from multiple sources; and

11.2.3 making, supplying or obtaining malware (malicious software), such as viruses, spyware, ransomware, botnets and Remote Access Trojans with the intent to commit further offence, including those above.

11.3 DET and its Schools are aware that pupils with particular skill and interest in computing and technology may inadvertently or deliberately stray into cyber-dependent crime.

11.4 DET and its Schools will take appropriate action to meet the cyber security standards to improve resilience against cyber-attacks.

11.5 If staff have any concerns about a child in this area, they should refer the matter to the DSL immediately. The DSL should then consider referring into the Cyber Choices programme. This is a nationwide police programme supported by the Home Office and led by the National Crime Agency, working with regional and local policing. It aims to intervene where young people are at risk of committing, or being drawn into, low-level cyber-dependent offences and divert them to a more positive use of their skills and interests. Cyber Choices does not currently cover "cyber-enabled" crime, such as fraud, purchasing of illegal drugs online and child sexual abuse and exploitation, nor other areas of concern such as online bullying or general online safety.

12 Risk Assessment

12.1 DET and its Schools recognise that technology, and the risks and harms associated with it, evolve and change rapidly. DET and its Schools will undertake regular, and, at least, annual, reviews of its approach to online safety, supported by risk assessments, which consider and reflect the risks faced by their pupils.

12.2 Furthermore, where a concern about a pupil's welfare is identified, the risks to that pupil's welfare will be assessed and appropriate action will be taken to reduce the risks identified.

12.3 Day-to-day responsibility to undertake risk assessments under this Policy will be delegated to the DSL, who has been properly trained in, and tasked with, carrying out the particular assessment.

13 Record Keeping

13.1 The DSL will review the records in order to evaluate all data recorded in order to meet their obligations under this Policy and establish trends (for example, in respect of particular socio-economic groups, or groups with a protected characteristic).

13.2 The information created in connection with this Policy may contain personal data. The use of this personal data by DET and its School will be in accordance with Data Protection law. DET has published Privacy Notices on its website, which apply to all DET Schools and explain how DET and its Schools will use personal data.

13.3 All records created in accordance with this Policy are managed in accordance with the DET Records Management Policy and DET Retention Schedules.

14 Publication, Availability and Feedback

14.1 This Policy is published on the DET website.

14.2 This Policy is available in hard copy on request, including in accessible formats.

14.3 A hard copy of the Policy is also available for inspection from the relevant School Office during the School day.

14.4 DET and its Schools welcome feedback on how this Policy can continue to improve. This feedback can be sent to the relevant School Office, marking the subject line "Feedback on the Online Safety Policy."

Appendix 1 Regulatory Framework

1 Regulatory Framework

1.1 This Policy has been prepared to meet the DET and its Schools' responsibilities under:

1.1.1 Education (Independent School Standards) Regulations 2014;

1.1.2 EYFS statutory framework for group and school-based providers (DfE, September 2025);

1.1.3 Education and Skills Act 2008;

1.1.4 Children Act 1989;

1.1.5 Childcare Act 2006;

1.1.6 Data Protection Act 2018 and UK General Data Protection Regulation (UK GDPR);

1.1.7 Data (Use and Access) Act 2025; and

1.1.8 Equality Act 2010.

1.2 This Policy has regard to the following guidance and advice:

Online Safety:

1.2.1 Keeping children safe in education (DfE, July 2026) (**KCSIE**)

1.2.2 Preventing and tackling bullying (DfE, July 2026);

1.2.3 Sharing nudes and semi-nudes: advice for education settings working with children and young people (Department for Science, Innovation & Technology (**DSIT**) and UK Council for Internet Safety (**UKCIS**), March 2024);

1.2.4 Prevent duty guidance for England and Wales (Home Office, March 2024);

1.2.5 The key principles of Prevent (Home Office, February 2026)

1.2.6 Channel duty guidance: protecting people susceptible to radicalisation (Home Office, October 2025);

1.2.7 Mobile phones in schools (DfE, January 2026);

1.2.8 Safeguarding children and protecting professionals in early years settings: online safety considerations (UKCIS, February 2019);]

1.2.9 Meeting digital and technology standards in education (DfE, maintained);

1.2.10 Plan technology for your school (HM Government, November 2025);

1.2.11 Teaching online safety in schools (DfE, January 2023);

1.2.12 Generative AI: product safety expectations (DfE, January 2026);

1.2.13 Using AI in education settings: support materials (DfE, May 2026)

1.2.14 Harmful online challenges and online hoaxes (DfE, February 2021);

1.2.15 Online safety guidance if you own or manage an online platform (DSIT, June 2021);

1.2.16 A business guide for protecting children on your online platform (DSIT, June 2021);

1.2.17 Online safety in schools and colleges: questions from the governing body (UKCIS, October 2022)

1.2.18 Online safety audit tool (UKCIS, October 2022);

1.2.19 Appropriate filtering for education settings (UKSIC, May 2025);

1.2.20 Appropriate monitoring for education settings (UKSIC, May 2025);

1.2.21 Online safety self-review tool for schools, 360safe.

Pupil Behaviour:

1.2.22 Searching, screening and confiscation: advice for schools (DfE, July 2023);

1.2.23 Behaviour in schools: advice for headteachers and school staff (DfE, February 2024)

Related guidance:

1.2.1 Relationships education, relationships and sex education (RSE) and health education (DfE, December 2025).[4]

[4] For teaching until 2026. From 2026 onwards refer to: Relationships education, relationships and sex education and health education guidance (from 1 September 2026).

Appendix 2 Other Relevant Policies

2 DET and its Schools have developed this Policy and the policies, procedures and resource materials that are relevant to this Policy as detailed below:

2.1 DET Acceptable Personal Use of Resources and Assets Policy (for staff);

2.2 DET Safeguarding and Child Protection Policy and local School procedures;

2.3 School Anti-Bullying Policy;

2.4 School Behaviour Policy;

2.5 DET Risk Assessment Policy for Pupil Welfare;

2.6 DET Staff Code of Conduct;

2.7 DET Whistleblowing Policy;

2.8 DET Data Protection Policy (for staff);

2.9 DET Information Governance suite of policies;

2.10 School Relationships and Sex Education Policy;

2.11 DET Generative AI Policy.