Delta Schools

E-Safety Policy

Policy /Procedure / Statement Title:	ESafety
Version:	1
Date published:	December 2024
Date to be reviewed by:	December 2026
Role of Reviewer:	Headteacher
Statutory (Y/N):	Y
Published on website: *	1A
Policy Level: **	2
Relevant to:	Students
Produced in consultation with:	Headteacher
Approved by:	Local School Board
Approval date:	2nd December 2024

*Publication on website			
Denbigh Alliance website		School website	
1	Statutory publication	A	Statutory publication
2	Good practice	B	Good practice
3	Not required	C	Not required

**Policy level			
1	Trust wide	Single policy relevant to everyone and consistently applied across all schools and departments, with no variation. e.g. Complaints procedure	Statutory policies approved by the Denbigh Alliance Board of Trustees (or designated Trustee Committee). Non-statutory policies approved by the CEO with exception of Executive Pay.
2	Trust core values	This policy defines the Trust core values in the form of a Trust statement to be incorporated fully into all other policies on this subject, that in addition contain relevant information, procedures and or processes contextualised to that school. e.g. Safeguarding, Behaviour	Statements in statutory policies approved by the Denbigh Alliance Board of Trustees (or designated Trustee Committee). Statements in non-statutory polices approved by the CEO. Policy approved by Local School Board.
3	School/department	These policies/procedures are defined independently by schools as appropriate. E.g. Anti-bullying	Approved by Local School Board.

1. Aims

The Delta Federation understands that using online services is an important aspect of raising educational standards, promoting pupil achievement, and enhancing teaching and learning. The use of online services is embedded throughout the schools in the Delta Federation; therefore, there are a number of controls in place to ensure the safety of pupils and staff.
The breadth of issues classified within online safety is considerable, but they can be categorised into four areas of risk:

- **Content**: Being exposed to illegal, inappropriate or harmful material, e.g. pornography, fake news, self-harm and suicide, and discriminatory or extremist views.
- **Contact**: Being subjected to harmful online interaction with other users, e.g. peer pressure, commercial advertising, and adults posing as children or young adults with the intention to groom or exploit children.
- **Conduct**: Personal online behaviour that increases the likelihood of, or causes, harm, e.g. sending and receiving explicit messages, and cyberbullying.
- **Commerce**: Risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

The measures implemented to protect pupils and staff revolve around these areas of risk. Our schools (Brooksward and Drayton Park) have created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff.

Our schools aim to:
Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

2. Legislation and guidance

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

- Voyeurism (Offences) Act 2019
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- DfE (2023) 'Filtering and monitoring standards for schools and colleges'
- DfE (2021) 'Harmful online challenges and online hoaxes'
- DfE (2023) 'Keeping children safe in education 2023'
- DfE (2023) 'Teaching online safety in school'
- DfE (2022) 'Searching, screening and confiscation'
- DfE (2023) 'Generative artificial intelligence in education'
- Department for Digital, Culture, Media and Sport and UK Council for Internet Safety (2020) 'Sharing nudes and semi-nudes: advice for education settings working with children and young people'
- UK Council for Child Internet Safety (2020) 'Education for a Connected World – 2020 edition'
- National Cyber Security Centre (2020) 'Small Business Guide: Cyber Security'

This policy operates in conjunction with the following school policies:

- Allegations of Abuse Against Staff Policy
- Child Protection and Safeguarding Policy
- Attitudes and Behaviour policy
- Anti-Bullying Policy
- Staff Code of Conduct
- Acceptable Use Policy
- Home-School Agreement
- Data protection policy and privacy notices
- Complaints procedure
- Remote Learning Policy

3. Roles and responsibilities

3.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the Executive Headteacher to account for its implementation.
The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governor who oversees online safety is Shanie Jamieson – shanie.jamieson@deltafederation.org.uk

All governors will:

- Ensure that they have read and understand this policy
- Ensuring that this policy is effective and complies with relevant laws and statutory guidance.
- Ensuring the DSL's remit covers online safety.
- Reviewing this policy on an **annual** basis.
- Ensuring their own knowledge of online safety issues is up-to-date.
- Ensuring all staff undergo safeguarding and child protection training, including online safety, at induction and at regular intervals.
- Ensuring that there are appropriate filtering and monitoring systems in place.
- Ensuring that the effectiveness of filtering and monitoring systems is reviewed at least annually in liaison with ICT staff and service providers.
- Ensuring that the SLT and other relevant staff have an awareness and understanding of the filtering and monitoring provisions in place, and manage them effectively and know how to escalate concerns when identified.
- Ensuring that all relevant school policies have an effective approach to planning for, and responding to, online challenges and hoaxes embedded within them.
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 2)

3.2 The headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school:

- Ensuring that online safety is a running and interrelated theme throughout the school's policies and procedures, including in those related to the curriculum, teacher training and safeguarding.
- Supporting the DSL and the deputy DSLs by ensuring they have enough time and resources to carry out their responsibilities in relation to online safety.
- Ensuring staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and safeguarding training.
- Ensuring online safety practices are audited and evaluated.
- Organising engagement with parents to keep them up-to-date with current online safety issues and how the school is keeping pupils safe.
- Working with the DSL and ICT technicians to conduct **half-termly** light-touch reviews of this policy.
- Working with the DSL and governing board to update this policy on an **annual** basis.

3.3 The designated safeguarding lead/E-Safety lead

Details of the school's designated safeguarding lead (DSL) and team are set out in our child protection and safeguarding policy.
The DSL alongside the E-Safety lead takes lead responsibility for online safety in school, in particular:

- Supporting the Heads of School and Executive Headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Executive Headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
- Ensuring online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented.
- Ensuring safeguarding is considered in the school's approach to remote learning.
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by pupils and staff, and ensuring all members of the school community understand this procedure.
- Understanding the filtering and monitoring processes in place at the school.

- Ensuring that all safeguarding training given to staff includes an understanding of the expectations, roles and responsibilities in relation to filtering and monitoring systems at the school (appendix 3 contains a self-audit for staff on online safety training needs).
- Maintaining records of reported online safety concerns or cyber-bullying as well as the actions taken in response to concerns in line with the school behaviour policy
- Monitoring online safety incidents to identify trends and any gaps in the school's provision, and using this data to update the school's procedures.
- Reporting to the governing board about online safety on a **termly** basis.
- Working with the Executive Headteacher and ICT technicians to conduct **half-termly** light-touch reviews of this policy.
- Working with the Executive Headteacher and governing board to update this policy on an **annual** basis.
- Liaising with other agencies and/or external services if necessary

This list is not intended to be exhaustive.

3.4 The ICT manager

The ICT manager is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a weekly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Working with the DSL and Executive Headteacher to conduct **half-termly** light-touch reviews of this policy

This list is not intended to be exhaustive.

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Taking responsibility for the security of ICT systems and electronic data they use or have access to.
- Modelling good online behaviours.
- Maintaining a professional level of conduct in their personal use of technology.
- Having an awareness of online safety issues.
- Ensuring they are familiar with, and understand, the indicators that pupils may be unsafe online.
- Maintaining an understanding of this policy, implementing it consistently.
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 2), and ensuring that pupils follow the school's terms on acceptable use (appendix 1)
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum.

This list is not intended to be exhaustive.

3.6 Pupils

Pupils will be responsible for:

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

3.7 Parents

Parents are expected to:

- Notify a member of staff, Head of School or the Executive Headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendix 1)

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

What are the issues?, UK Safer Internet Centre: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues
Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics
Parent factsheet, Childnet International: http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf

3.8 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 2).

4. Managing online safety

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

The DSL and E-Safety lead have overall responsibility for the school's approach to online safety, with support from deputies and the Executive Headteacher where appropriate, and will ensure that there are strong processes in place to handle any concerns about pupils' safety online. The DSL should liaise with the police or children's social care services for support responding to harmful online sexual behaviour.

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

- Staff and governors receive regular training
- Staff receive regular email updates regarding online safety information and any changes to online safety guidance or legislation
- Online safety is integrated into learning throughout the curriculum
- Assemblies are conducted termly on the topic of remaining safe online

Handling online safety concerns

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

Staff will be aware that harmful online sexual behaviour can progress on a continuum, and appropriate and early intervention can prevent abusive behaviour in the future. Staff will also acknowledge that pupils displaying this type of behaviour are often victims of abuse themselves and should be suitably supported. The victim of online harmful sexual behaviour may ask for no one to be told about the abuse. The DSL will consider whether sharing details of the abuse would put the victim in a more harmful position, or whether it is necessary in order to protect them from further harm. Ultimately the DSL will balance the victim's wishes against their duty to protect the victim and other young people. The DSL and other appropriate staff members will meet with the victim's parents to discuss the safeguarding measures that are being put in place to support their child and how the report will progress.

Confidentiality will not be promised, and information may be still shared lawfully, for example, if the DSL decides that there is a legal basis under UK GDPR such as the public task basis whereby it is in the public interest to share the information. If the decision is made to report abuse to children's social care or the police against the victim's wishes, this must be handled extremely carefully – the reasons for sharing the information should be explained to the victim and appropriate specialised support should be offered. Concerns regarding a staff member's online behaviour are reported to the Executive Headteacher, who decides on the best course of action in line with the relevant policies. If the concern is about the Executive Headteacher, it is reported to the chair of governors.

Concerns regarding a pupil's online behaviour are reported to the DSL, who investigates concerns with relevant staff members, e.g. the Executive Headteacher and ICT technicians, and manages concerns in

accordance with relevant policies depending on their nature, e.g. the Attiudes and Behaviour Policy and Child Protection and Safeguarding Policy.

Where there is a concern that illegal activity has taken place, the Executive Headteacher contacts the police. The school avoids unnecessarily criminalising pupils, e.g. calling the police, where criminal behaviour is thought to be inadvertent and as a result of ignorance or normal developmental curiosity, e.g. a pupil has taken and distributed indecent imagery of themselves. The DSL will decide in which cases this response is appropriate and will manage such cases in line with the Child Protection and Safeguarding Policy.

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

5. Cyberbullying

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

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

Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the Attitudes and Behaviour policy.)

The school will be aware that certain pupils can be more at risk of abuse and/or bullying online, such as LGBTQ+ pupils and pupils with SEND.
Cyberbullying against pupils or staff is not tolerated under any circumstances. Incidents of cyberbullying are dealt with quickly and effectively wherever they occur in line with the Anti-Bullying Policy.

Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.
The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their tutor groups, and the issue will be addressed in assemblies.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).
In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

6. Child-on-child sexual abuse and harassment

Pupils may also use the internet and technology as a vehicle for sexual abuse and harassment. Staff will understand that this abuse can occur both in and outside of school, off and online, and will remain aware that

pupils are less likely to report concerning online sexual behaviours, particularly if they are using websites that they know adults will consider to be inappropriate for their age.
The following are examples of online harmful sexual behaviour of which staff will be expected to be aware:

- Threatening, facilitating or encouraging sexual violence
- Upskirting, i.e. taking a picture underneath a person's clothing without consent and with the intention of viewing their genitals, breasts or buttocks
- Sexualised online bullying, e.g. sexual jokes or taunts
- Unwanted and unsolicited sexual comments and messages
- Consensual or non-consensual sharing of sexualised imagery
- Abuse between young people in intimate relationships online

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

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

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

The school will respond to all concerns regarding online child-on-child sexual abuse and harassment, regardless of whether the incident took place on the school premises or using school-owned equipment.

Concerns regarding online child-on-child abuse will be reported to the DSL, who will investigate the matter in line with the Attitudes and Behaviour policy.

7. Grooming and exploitation

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

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

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

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

Child sexual exploitation (CSE) and child criminal exploitation (CCE)

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

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

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

Radicalisation

Radicalisation is the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups. This process can occur through direct recruitment, e.g. individuals in extremist groups identifying, targeting and contacting young people with the intention of involving them in terrorist activity, or by exposure to violent ideological propaganda. Children who are targets for radicalisation are likely to be groomed by extremists online to the extent that they believe the extremist has their best interests at heart, making them more likely to adopt the same radical ideology.

Staff members will be aware of the factors which can place certain pupils at increased vulnerability to radicalisation, as outlined in the Prevent Duty section of the Child Protection Polcy. Staff will be expected to exercise vigilance towards any pupils displaying indicators that they have been, or are being, radicalised. Where staff have a concern about a pupil relating to radicalisation, they will report this to the DSL without delay, who will handle the situation in line with the Child Protection Policy.

8. Mental health

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

9. Online hoaxes and harmful online challenges

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

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

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

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

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

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

- Supportive.
- In line with the Child Protection and Safeguarding Policy.

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

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

10. Cyber-crime

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

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

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

The DSL, Executive Headteacher and Heads of School will ensure that pupils are taught, throughout the curriculum, how to use technology safely, responsibly and lawfully.

11. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum.
In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact
- The safe use of social media and the internet is covered in Appendix 3

The safe use of social media and the internet will also be covered in other subjects where relevant. See Appendix 3 for more information.

The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

12. Educating parents about online safety

The school will work in partnership with parents to ensure pupils stay safe online at school and at home. Parents will be provided with information about the school's approach to online safety and their role in protecting their children. Parents will be sent a copy of the Acceptable Use Agreement at when their child joins one of the schools in the Delta Federation and are encouraged to regularly go through this with their child to ensure their child understands the document and the implications of not following it.

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

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

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

Parental awareness regarding how they can support their children to be safe online will be raised in the following ways:

- Regular letters or other communications home
- Parents' evenings
- Parent presentations and workshops
- Newsletters
- Online resources shared on the school websites

If parents have any queries or concerns in relation to online safety or this policy, these should be raised in the first instance with the Head of School, Executive Headteacher and/or the DSL.

13. Online safety training for staff

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

14. Online safety and the curriculum

Online safety is embedded throughout the curriculum; however, it is particularly addressed in the following subjects:

- Relationships and health education
- PSHE
- Citizenship
- ICT

Online safety teaching is always appropriate to pupils' ages and developmental stages.
Pupils are taught the underpinning knowledge and behaviours that can help them to navigate the online world safely and confidently regardless of the device, platform or app they are using. The underpinning knowledge and behaviours pupils learn through the curriculum include the following:

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

The online risks pupils may face online are always considered when developing the curriculum. The risks that are considered and how they are covered in the curriculum can be found in appendix 5 of this policy.

The DSL and E-Safety lead will be involved with the development of the school's online safety curriculum. Pupils will be consulted on the online safety curriculum, where appropriate, due to their unique knowledge of the kinds of websites they and their peers frequent and the kinds of behaviours in which they engage online. Relevant members of staff, e.g. the SENCO and designated teacher for LAC, will work together to ensure the curriculum is tailored so that pupils who may be more vulnerable to online harms, e.g. pupils with SEND and LAC, receive the information and support they need.

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

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

External visitors may be invited into school to help with the delivery of certain aspects of the online safety curriculum. The Executive Headteacher, Heads of School and DSL will decide when it is appropriate to invite external groups into school and ensure the visitors selected are appropriate.

Before conducting a lesson or activity on online safety, the class teacher and DSL will consider the topic that is being covered and the potential that pupils in the class have suffered or may be suffering from online abuse or harm in this way. The DSL will advise the staff member on how to best support any pupil who may be especially impacted by a lesson or activity. Lessons and activities will be planned carefully so they do not draw attention to a pupil who is being or has been abused or harmed online, to avoid publicising the abuse. During an online safety lesson or activity, the class teacher will ensure a safe environment is maintained in which pupils feel comfortable to say what they feel and ask questions, and are not worried about getting into trouble or being judged.

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

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

15. Use of technology in the classroom

A wide range of technology will be used during lessons, including the following:
- Computers
- Laptops
- Tablets and iPads
- Email
- Cameras

Prior to using any websites, tools, apps or other online platforms in the classroom, or recommending that pupils use these platforms at home, the class teacher will review and evaluate the resource. Class teachers will ensure that any internet-derived materials are used in line with copyright law.
Pupils will be supervised when using online materials during lesson time – this supervision is suitable to their age and ability.

16. Use of smart technology

While the schools in the Delta Federation recognise that the use of smart technology can have educational benefits, there are also a variety of associated risks which the school will ensure it manages.

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

Staff will use all smart technology and personal technology in line with the school's Acceptable Use Policy. The school recognises that pupils' unlimited and unrestricted access to the internet via mobile phone networks means that some pupils may use the internet in a way which breaches the school's acceptable use of ICT agreement for pupils.

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

Pupils will not be permitted to use smart devices or any other personal technology whilst in school; mobile phones must be handed in to the school office at the beginning of the day and collected from the office at the end of the school day.

Where there is a significant problem with the misuse of smart technology among pupils, the school will discipline those involved in line with the school's Attitudes and Behaviour Policy.

The school will hold assemblies, where appropriate, which address any specific concerns related to the misuse of smart technology and outline the importance of using smart technology in an appropriate manner. The school will seek to ensure that it is kept up to date with the latest devices, platforms, apps, trends and related threats.

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

17. Internet access

Pupils, staff and other members of the school community will only be granted access to the school's internet network once they have read and signed the Acceptable Use Agreement. A record will be kept of users who have been granted internet access in the school office.
All members of the school community will be encouraged to use the school's internet network, instead of 3G, 4G and 5G networks, as the network has appropriate filtering and monitoring to ensure individuals are using the internet appropriately.

18. Filtering and monitoring online activity

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

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

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

Requests regarding making changes to the filtering system will be directed to the Executive Headteacher, Heads of School or E-Safety Lead. Prior to making any changes to the filtering system, ICT technicians and the DSL will conduct a risk assessment. Any changes made to the system will be recorded by ICT technicians. Reports of inappropriate websites or materials will be made to an ICT technician immediately, who will investigate the matter and makes any necessary changes.

Deliberate breaches of the filtering system will be reported to the DSL and ICT technicians, who will escalate the matter appropriately. If a pupil has deliberately breached the filtering system, they will be disciplined in line with the Behaviour Policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate. If a member of staff has deliberately breached the filtering system, they will be disciplined in line with the Disciplinary Policy and Procedure.

If material that is believed to be illegal is accessed, inadvertently or deliberately, this material will be reported to the appropriate agency immediately, e.g. the Internet Watch Foundation (IWF), CEOP and/or the police. The school's network and school-owned devices will be appropriately monitored. All users of the network and school-owned devices will be informed about how and why they are monitored. Concerns identified through monitoring will be reported to the DSL who will manage the situation in line with the Child Protection and Safeguarding Policy.

19. Network security

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

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

All members of staff will have their own unique usernames and private passwords to access the school's systems. Pupils in key stage 2 will be provided with their own unique username and private passwords. Staff members and pupils will be responsible for keeping their passwords private. Passwords will have a minimum and maximum length and require a mixture of letters, numbers and symbols to ensure they are as secure as possible. Staff passwords will expire after **90** days after which users will be required to change them.

Users will inform ICT technicians if they forget their login details, who will arrange for the user to access the systems under different login details. Users will not be permitted to share their login details with others and will not be allowed to log in as another user at any time. If a user is found to be sharing their login details or otherwise mistreating the password system, the Executive Headteacher will be informed and will decide the necessary action to take.

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

20. Emails

Access to and the use of emails will be managed in line with the Data Protection Policy, Acceptable Use Agreement, and the Pupil Confidentiality Policy and Staff and Volunteer Confidentiality Policy.

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

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

21. Generative artificial intelligence (AI)

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

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

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

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

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

22. The school website

The Executive Headteacher will be responsible for the overall content of the school website – they will ensure the content is appropriate, accurate, up-to-date and meets government requirements.
The website will be managed in line with the School Website Policy.

23. Use of devices

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

The use of personal devices on the school premises and for the purposes of school work will be managed in line with the Staff Acceptable Use policy.

24. Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

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

25. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 2.

This policy will be reviewed biennially by the Teaching and Learning Committee. At every review, the policy will be shared with the governing board.

Appendix 1: Acceptable use agreement (pupils and parents/carers)

Acceptable use of the school's ICT systems and internet: agreement for pupils and parents/carers	
Name of pupil:	
When using the school's ICT systems and accessing the internet in school, I will not: Use them for a non-educational purpose Use them without a teacher being present, or without a teacher's permission Access any inappropriate websites Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity) Use chat rooms Open any attachments in emails, or follow any links in emails, without first checking with a teacher Use any inappropriate language when communicating online, including in emails Share my password with others or log in to the school's network using someone else's details Give my personal information (including my name, address or telephone number) to anyone without the permission of my teacher or parent/carer Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision If I bring a personal mobile phone or other personal electronic device into school: I will hand it in to the school office before going to class at the start of the school day I will collect it from the school office after being dismissed from class at 3:15pm I will not use it during lessons, tutor group time, clubs or other activities organised by the school, without a teacher's permission I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online I agree that the school will monitor the websites I visit. I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others. I will always use the school's ICT systems and internet responsibly.	
Signed (pupil):	**Date:**
Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 2: Online safety incident report log

Online safety incident report log				
Date	**Where the incident took place**	**Description of the incident**	**Action taken**	**Name and signature of staff member recording the incident**

Appendix 3: Child Focused E-Safety Protocol

1. Educating pupils about online safety
Pupils will be taught about online safety as part of the curriculum.
In **Key Stage 1**, pupils will be taught to:

- To know there are unfamiliar people online and to consider them unsafe
- To treat others online kindly and with respect
- Use technology safely and respectfully, keeping personal information private
- Know where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage 2** will be taught to:

- To ensure personal and private information is never shared online
- Use technology safely, respectfully and responsibly
- To show and promote kind and respectful treatment of others online
- Consider the digital footprint a user leaves online
- Recognise acceptable and unacceptable behavior in a variety of digital environments
- Identify and use a range of ways to report concerns about content and contact
- To share and encourage other students to use safe and responsible practices online

The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.
Pupils will complete a half term unit of e-safety related learning each school year. This may be embedded within other learning or discreetly taught as a specific unit of work.
E-Safety is the responsibility of everyone in and around the school community. The role of the safeguarding team is to support and lead all members of the community in safe and responsible online activity.

Responsible and Respectful
Children are expected to learn about and embody a responsible and respectful attitude to all online behavior, in and outside of school. This mentality will be developed through discreet teaching, modelling by teachers and older peers and a narrative of appropriate activity and behavior within assemblies, safer internet week and daily practice in classroom settings.

Data Protection and Privacy
Children will be taught to understand that some information and data is private and should not be shared. It is crucial children know what data is private to them and others so they can protect themselves at all times. Children need to be encouraged to consider their own digital footprint and the traces their activities leaves online. Consequently, children must know what to do, or be supported in acting, should any loss or accidental sharing of theirs or someone else's data.
Privacy is critical in protecting one's personal data, this must be explicit to children throughout any discreet teaching or information pertaining to online safety. Children will be encouraged to always maintain the highest levels of any privacy settings online; as part of any account; activity or use of websites. It is important that this is reflected by all staff, as per the *Brooksward School Online Safety Policy.*

Cyberbullying
Children will be taught the definition of Cyberbullying as it appears in the *Brooksward School Online Safety Policy* and will be made aware of how to raise concerns with school staff should they be involved in any such incident. They will also be made aware of how situations will be dealt with, as per the *Brooksward School Behaviour Policy.*

Age Restrictions
It is expected that children comply with age restrictions and recommendations in place on all websites and digital media for use online (including, but not limited to: social media websites, YouTube, email accounts, PlayStation Network, Microsoft XboxLive, computer and console games, videos, Blu-Ray, DVD). Parents and carers should be asked and encouraged to support the school community in adhering to any age restriction relating to online content and activity. Issues relating to children's non-compliance to any age restriction or recommendation will be dealt with as per the *Brooksward School Behaviour Policy*.

Appendix 4
We ask all of our families to sign a copy of the Remote Learning Agreement

Remote Learning Agreement - children who are working remotely and in school

We ask all children, young people and adults involved in the life of Brooksward School/Drayton Park School to sign this Remote Learning Agreement to outline how we expect them to behave when they are online, and/or using school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).

Your children should not behave any differently when they are out of school or using their own device or home network than they would in the classroom whilst completing remote learning.

The rules around behaviour and respect for pupils applies to all members of the school community, whether they are at home or school whilst they are carrying out their learning.

You can read the full Remote Learning Policy on our website for more details on our approach to online safety and links to other relevant policies (e.g. Safeguarding Policy, Behaviour Policy, etc).

If you have any questions about this RLA or our approach to online safety, please contact the school.

Parent/carers and each child must read the following guidance and agree to the conditions.

Parent/Carer Agreement

1. I understand that Brooksward/Drayton Park School uses technology as an approach to their remote learning whilst pupils are unable to attend school.

2. I understand that the school takes every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials, including behaviour policies and agreements and internet safety education. However, the school cannot be held responsible for the nature and content of materials accessed through the internet and mobile technologies at home, which can sometimes be upsetting.

3. I understand that the video and microphone will be on and others on the virtual session will be able to see and hear my child when we are engaged in a class group session.

4. I will promote positive online safety and model safe, responsible and positive behaviours in my own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, pupils or other parents/carers.

5. I understand that for my child to grow up safe online, s/he will need positive input from school and home, so I will talk to my child about online safety.

6. I understand that my child needs a safe and appropriate place to do remote learning if school or bubbles are closed. When on any live video calls with school, my child will be fully dressed and in a space where there are able to concentrate, a clear background and the camera angle will point away from any personal information/photographs etc. Where it is possible to blur or change the background, I will help my child to do so.

7. I understand that whilst home networks are much less secure than school ones, I can apply child safety settings to my home internet. Internet Matters provides guides to help parents do this easily for all the main internet service providers in the UK. There are also child-safe search engines e.g. swiggle.org.uk

8. I understand that I am responsible for supervising my child's access to virtual calls and will monitor my child during this time and take responsibility for their conduct. I understand that I am not part of the learning session and will be there to support my child with their technology, where appropriate. I will ensure that they are ready for their live learning session.

9. I understand that each virtual meeting will end at the discretion of the teacher and that children may face future sanctions such as being blocked or removed from calls if they do not follow this agreement.

10. I understand that virtual sessions will be recorded by class teachers and may be saved according to data protection guidelines and safeguarding.

11. I understand that I must not take any photographs or videos of the live session myself.

12. I understand that teachers or support staff will lead and facilitate all virtual meetings and that classroom behaviour and rules will be followed by my child during this time.

13. I understand that I must maintain confidentiality of the content of the virtual sessions and not share any information about it verbally or online.

14. I understand if I am concerned about anything that happens in the live session, I must report it to the class teacher or Head.

Child Agreement

Please share this with your child so they know what they must do to keep themselves safe online.

1.When I learn online – I use technological devices and logins for remote learning, other activities and having fun. All of my devices and systems are monitored by an adult when I'm using them at home.

2. When I am completing my home learning, I follow the school values

3. I will only use devices, apps, sites and games that are age appropriate when I am allowed to.

4. I am a friend online – I won't share or say anything that I know would upset another person or they wouldn't want shared. If a friend is worried or needs help, I remind them to talk to an adult, or even do it for them.

5. I am a secure online learner – I keep my passwords to myself and reset them if anyone finds them out. Friends don't share passwords!

6. I am careful what I click on – I don't click on unexpected links or popups, and only download or install things when I know it is safe or has been agreed by trusted adults. Sometimes app add-ons can cost money, so it is important I always check.

7. I ask for help if I am scared or worried by something I see– I will talk to a trusted adult if anything upsets me or worries me on an app, site or game.

When I am on live learning sessions I will:

- be ready to learn including going to the toilet before the session
- dress appropriately

- I am in a safe and calm place at home which is a suitable space for my teachers to call me in.

- I will follow the school values at all times and use kind words towards others during calls.

- I will listen and follow the instructions of the class teacher during calls in the same way I would in the classroom.

- If I have a question, my teacher will let me know how I can do this

- I will be ready for my learning with the resources I need (paper, pencil, online resource)

- I will complete all work set as well as I possibly can

If I have any questions about this, I will ask my family or teacher.

Child Agreement: I have shared this with my child and they have understood this agreement
YES
Child Name

Parent/Carer Agreement: I have read and agree to all terms
YES
Adult Name Signed

Curriculum coverage (Appendix 5) – Note to self: need to check what the colours mean

Year One – E-Safety	**1. Self-Image and Identity**	**2. Online Relationships**	**3. Online Reputation**	**4. Online Bullying**	**5. Managing Online Information**	**6. Health, Wellbeing and Lifestyle**	**7. Privacy and Security**	**8. Copyright and Ownership**
	I can recognise that there may be people online who could make me feel sad, embarrassed or upset. If something happens that makes me feel sad, worried, uncomfortable or frightened I can give examples of when and how to speak to an adult I can trust.	I can use the internet with adult support to communicate with people I know. I can explain why it is important to be considerate and kind to people online. Knows the internet can be used to communicate with other people.	I can recognise that information can stay online and could be copied. I can describe what information I should not put online without asking a trusted adult first.	I can describe how to behave online in ways that do not upset others and can give examples.	I can use the internet to find things out. I can use simple keywords in search engines. I can describe and demonstrate how to get help from a trusted adult or helpline if I find content that makes me feel sad, uncomfortable worried or frightened.	I can identify rules that help keep us safe and healthy in and beyond the home when using technology. I can explain rules to keep us safe when we are using technology both in and beyond the home. I can give examples of some of these rules.	I can recognise more detailed examples of information that is personal to me (e.g. where I live, my family's names, where I go to school). I can explain why I should always ask a trusted adult before I share any information about myself online. I can explain how passwords can be used to protect information and devices.	I can explain why work I create using technology belongs to me. I can say why it belongs to me (e.g. 'it is my idea' or 'I designed it'). I can save my work so that others know it belongs to me (e.g. filename, name on content).
Year Two – E-Safety	**1. Self-Image and Identity**	**2. Online Relationships**	**3. Online Reputation**	**4. Online Bullying**	**5. Managing Online Information**	**6. Health, Wellbeing and Lifestyle**	**7. Privacy and Security**	**8. Copyright and Ownership**
	I can explain how other people's identity online can be different to their identity in real life. I can describe ways in which people might make themselves look different online. I can give examples of issues online that might make me feel sad, worried, uncomfortable or frightened; I can give examples of how I might get help.	I can use the internet to communicate with people I don't know well (e.g. email a penpal in another school/ country). I can give examples of how I might use technology to communicate with others I don't know well.	I can explain how information put online about me can last for a long time. I know who to talk to if I think someone has made a mistake about putting something online.	I can give examples of bullying behaviour and how it could look online. I understand how bullying can make someone feel. I can talk about how someone can/would get help about being bullied online or offline.	I can use keywords in search engines. I can demonstrate how to navigate a simple webpage to get to information I need (e.g. home, forward, back buttons; links, tabs and sections). I can explain what voice activated searching is and how it might be used (e.g. Alexa, Google Now, Siri). I can explain the difference between things that are imaginary, 'made up' or 'make believe' and things that are 'true' or 'real'. I can explain why some	I can explain simple guidance for using technology in different environments and settings. I can say how those rules/guides can help me.	I can describe how online information about me could be seen by others. I can describe and explain some rules for keeping my information private. I can explain what passwords are and can use passwords for my accounts and devices. I can explain how many devices in my home could be connected to the internet and can list some of those devices.	I can describe why other people's work belongs to them. I can recognise that content on the internet may belong to other people.

					information I find online may not be true.			
Year Three – E-Safety	**1. Self-Image and Identity**	**2. Online Relationships**	**3. Online Reputation**	**4. Online Bullying**	**5. Managing Online Information**	**6. Health, Wellbeing and Lifestyle**	**7. Privacy and Security**	**8. Copyright and Ownership**
	I can explain what is meant by the term 'identity'. I can explain how I can represent myself in different ways online. I can explain ways in which and why I might change my identity depending on what I am doing online (e.g. gaming; using an **avatar**; social media).	I can describe ways people who have similar likes and interests can get together online. I can give examples of technology specific forms of communication (e.g. emojis, acronyms, text speak). I can explain some risks of communicating online with others I don't know well. I can explain why I should be careful who I trust online and what information I can trust them with. I can explain how my and other people's feelings can be hurt by what is said or written online. I can explain why I can take back my trust in someone or something if I feel nervous, uncomfortable or worried. I can explain what it means to 'know someone' online and why this might be different from knowing someone in real life. I can explain what is	I can search for information about myself online. I can recognize I need to be careful before I share anything about myself or others online. I know who I should ask if I am not sure if I should put something online.	I can explain what bullying is and can describe how people may bully others. I can describe rules about how to behave online and how I follow them.	I can use key phrases in search engines. I can explain what **autocomplete** is and how to choose the best suggestion. I can explain how the internet can be used to sell and buy things. I can explain the difference between a 'belief', an 'opinion' and a 'fact'.	I can explain why spending too much time using technology can sometimes have a negative impact on me. Can give some examples of activities where it is easy to spend a lot of time engaged (e.g. games, films, videos).	I can give reasons why I should only share information with people I choose to and can trust. I can explain that if I am not sure or I feel pressured, I should ask a trusted adult. I understand and can give reasons why passwords are important. I can describe simple strategies for creating and keeping passwords private. I can describe how connected devices can collect and share my information with others.	I can explain why copying someone else's work from the internet without permission can cause problems. I can give examples of what those problems might be.

		meant by 'trusting someone online'. I can explain why this is different from 'liking someone online'.						
Year Four – E-Safety	**1. Self-Image and Identity**	**2. Online Relationships**	**3. Online Reputation**	**4. Online Bullying**	**5. Managing Online Information**	**6. Health, Wellbeing and Lifestyle**	**7. Privacy and Security**	**8. Copyright and Ownership**
	I can explain how my online identity can be different to the identity I present in 'real life'. Knowing this, I can describe the right decisions about how I interact with others and how others perceive me.	I can describe strategies for safe and fun experiences in a range of online social environments. I can give examples of how to be respectful to others online.	I can describe how others can find out information about me by looking online. I can explain ways that some of the information about me online could have been created, copied or shared by others.	I can identify some online technologies where bullying might take place. I can describe ways people can be bullied through a range of media (e.g. image, video, text, **chat**). I can explain why I need to think carefully about how content I post might affect others, their feelings and how it may affect how others feel about them (their reputation).	I can analyse information and differentiate between 'opinions', 'beliefs' and 'facts'. I understand what criteria have to be met before something is a 'fact'. I can describe how I can search for information within a wide group of technologies (e.g. social media, image sites, video sites). I can describe some of the methods used to encourage people to buy things online (e.g. advertising offers; **in-app purchases**, pop-ups) and can recognise some of these when they appear online. I can explain that some people I 'meet online' (e.g. through social media) may be computer programmes pretending to be real people. I can explain why lots of people sharing the same opinions or beliefs online does not make those opinions or beliefs true.	I can explain how using technology can distract me from other things I might do or should be doing. I can identify times or situations when I might need to limit the amount of time I use technology. I can suggest strategies to help me limit this time.	I can explain what a strong password is. I can describe strategies for keeping my personal information private, depending on context. I can explain that others online can pretend to be me or other people, including my friends. I can suggest reasons why they might do this. I can explain how internet use can be monitored.	When searching on the internet for content to use, I can explain why I need to consider who owns it and whether I have the right to reuse it. I can give some simple examples.
Year Five –	**1. Self-Image and Identity**	**2. Online Relationships**	**3. Online Reputation**	**4. Online Bullying**	**5. Managing Online Information**	**6. Health, Wellbeing and Lifestyle**	**7. Privacy and Security**	**8. Copyright and Ownership**

E-Safety	I can explain how identity online can be copied, modified or altered. I can demonstrate responsible choices about my online identity, depending on context.	I can explain that there are some people I communicate with online who may want to do me or my friends harm. I can recognise that this is not my/our fault. I can make positive contributions and be part of online communities. I can describe some of the communities in which I am involved and describe how I collaborate with others positively.	I can search for information about an individual online and create a summary report of the information I find. I can describe ways that information about people online can be used by others to make judgments about an individual.	I can recognise when someone is upset, hurt or angry online. I can describe how to get help for someone that is being bullied online and assess when I need to do or say something or tell someone. I can explain how to block abusive users. I can explain how I would report online bullying on the apps and platforms that I use. I can describe the helpline services who can support me and what I would say and do if I needed their help (e.g. **Childline**).	I can use different search technologies. I can evaluate digital content and can explain how I make choices from search results. I can explain key concepts including: data, information, fact, opinion belief, true, false, valid, reliable and evidence. I understand the difference between online **mis-information** (inaccurate information distributed by accident) and **dis-information** (inaccurate information deliberately distributed and intended to mislead). I can explain what is meant by 'being sceptical'. I can give examples of when and why it is important to be 'sceptical'. I can explain what is meant by a '**hoax**'. I can explain why I need to think carefully before I forward anything online. I can explain why some information I find online may not be honest, accurate or legal. I can explain why information that is on a large number of sites may still be inaccurate or untrue. I can assess how this might happen (e.g. the sharing of misinformation either by accident or on purpose).	I can describe ways technology can affect healthy sleep and can describe some of the issues. I can describe some strategies, tips or advice to promote healthy sleep with regards to technology.	I can create and use strong and secure passwords. I can explain how many free apps or services may read and share my private information (e.g. friends, contacts, likes, images, videos, voice, messages, **geolocation**) with others. I can explain how and why some apps may request or take payment for additional content (e.g. in-app purchases) and explain why I should seek permission from a trusted adult before purchasing.	I can assess and justify when it is acceptable to use the work of others. I can give examples of content that is permitted to be reused.
Year Six –	**1. Self-Image and Identity**	**2. Online Relationships**	**3. Online Reputation**	**4. Online Bullying**	**5. Managing Online Information**	**6. Health, Wellbeing and Lifestyle**	**7. Privacy and Security**	**8. Copyright and Ownership**

E-Safety	I can describe ways in which media can shape ideas about gender. I can identify messages about gender roles and make judgements based on them. I can challenge and explain why it is important to reject inappropriate messages about gender online. I can describe issues online that might make me or others feel sad, worried, uncomfortable or frightened. I know and can give examples of how I might get help, both on and offline. I can explain why I should keep asking until I get the help I need.	I can show I understand my responsibilities for the well-being of others in my online social group. I can explain how impulsive and rash communications online may cause problems (e.g. flaming, content produced in live streaming). I can demonstrate how I would support others (including those who are having difficulties) online. I can demonstrate ways of reporting problems online for both myself and my friends.	I can explain how I am developing an online reputation which will allow other people to form an opinion of me. I can describe some simple ways that help build a positive online reputation.	I can describe how to capture bullying content as evidence (e.g **screen-grab**, **URL**, **profile**) to share with others who can help me. I can identify a range of ways to report concerns both in school and at home about online bullying.	I can use search technologies effectively. I can explain how search engines work and how results are selected and ranked. I can demonstrate the strategies I would apply to be discerning in evaluating digital content. I can describe how some online information can be opinion and can offer examples. I can explain how and why some people may present 'opinions' as 'facts'. I can define the terms 'influence', 'manipulation' and 'persuasion' and explain how I might encounter these online (e.g. advertising and 'ad targeting'). I can demonstrate strategies to enable me to analyse and evaluate the validity of 'facts' and I can explain why using these strategies are important. I can identify, flag and report inappropriate content.	I can describe common systems that regulate age-related content (e.g. **PEGI**, **BBFC**, parental warnings) and describe their purpose. I can assess and action different strategies to limit the impact of technology on my health (e.g. **night-shift mode**, regular breaks, correct posture, sleep, diet and exercise). I can explain the importance of self-regulating my use of technology; I can demonstrate the strategies I use to do this (e.g. monitoring my time online, avoiding accidents).	I use different passwords for a range of online services. I can describe effective strategies for managing those passwords (e.g. **password managers**, acronyms, stories). I know what to do if my password is lost or stolen. I can explain what app permissions are and can give some examples from the technology or services I use. I can describe simple ways to increase privacy on apps and services that provide privacy settings. I can describe ways in which some online content targets people to gain money or information illegally; I can describe strategies to help me identify such content (e.g. **scams**, **phishing**).	I can demonstrate the use of search tools to find and access online content which can be reused by others. I can demonstrate how to make references to and acknowledge sources I have used from the internet.