Dore Primary School

Online Safety Policy

Version	1.5
Author	Matt Smith (Updated June 2023)
Date Approved by Governing Body (annual)	17th July 2023
Review Date	July 2024

Signed by:

_____ Headteacher Date: _____

_____ Chair of governors Date: _____

Contents:

Statement of intent

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

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

- **Content**: Being exposed to illegal, inappropriate or harmful material, e.g. pornography, 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 school has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff.

As a Rights Respecting School, the best interests of the child are a top priority (article 3) and we ensure children know about their rights when thinking about relationships. These include the right to an education (article 28), protection from harm (article 19) and privacy (article 16).

1. [Updated] Legal framework

[Updated] 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 (2021) 'Harmful online challenges and online hoaxes'
- **[Updated]** DfE (2022) 'Keeping children safe in education 2022'
- DfE (2019) 'Teaching online safety in school'
- DfE (2018) 'Searching, screening and confiscation'
- 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 (2018) 'Small Business Guide: Cyber Security'

[Updated] This policy operates in conjunction with the following school policies:

- Social Media Policy
- Allegations of Abuse Against Staff Policy
- **[New]** Low-level Safeguarding Concerns Policy
- Acceptable Use Agreement
- Data and Cyber-security Breach Prevention and Management Plan
- Child Protection and Safeguarding Policy
- **[New]** Child-on-child Abuse Policy
- Anti-Bullying Policy
- PSHE Policy
- RSE and Health Education Policy
- Searching, Screening and Confiscation Policy
- Pupils' Personal Electronic Devices Policy
- Staff Code of Conduct
- Behaviour Policy
- Disciplinary Policy and Procedures
- Data Protection Policy
- Confidentiality Policy
- Photography Policy
- Device User Agreement
- Staff ICT and Electronic Devices Policy
- Prevent Duty Policy
- Pupil Remote Learning Policy
- Technology Acceptable Use Agreement for Pupils
- Technology Acceptable Use Agreement – Staff

2. [Updated] Roles and responsibilities

The governing board is responsible for:

- 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.
- Ensuring that there are appropriate filtering and monitoring systems in place.
- Ensuring that all relevant school policies have an effective approach to planning for, and responding to, online challenges and hoaxes embedded within them.

The headteacher is responsible for:

- Ensuring that online safety is a running and interrelated theme throughout the school's policies and procedures, including in those related to the curriculum, teacher training and safeguarding.
- Supporting the DSL and the deputy DSL by ensuring they have enough time and resources to carry out their responsibilities in relation to online safety.
- Ensuring staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and safeguarding training.
- Ensuring online safety practices are audited and evaluated.
- Supporting staff to ensure that online safety is embedded throughout the curriculum so that all pupils can develop an appropriate understanding of online safety.
- 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.

[Updated] The DSL is responsible for:

- Taking the lead responsibility for online safety in the school.
- Acting as the named point of contact within the school on all online safeguarding issues.
- Undertaking training so they understand the risks associated with online safety and can recognise additional risks that pupils with SEND face online.
- Liaising with relevant members of staff on online safety matters, e.g. the SENCO and ICT technicians.
- Ensuring online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented.
- Ensuring safeguarding is considered in the school's approach to remote learning.
- Ensuring appropriate referrals are made to external agencies, as required.
- **[New]** Working closely with the police during police investigations.
- Keeping up-to-date with current research, legislation and online trends.

- Coordinating the school's participation in local and national online safety events, e.g. Safer Internet Day.
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by pupils and staff.
- Ensuring all members of the school community understand the reporting procedure.
- Maintaining records of reported online safety concerns as well as the actions taken in response to concerns.
- Monitoring online safety incidents to identify trends and any gaps in the school's provision, and using this data to update the school's procedures.
- Reporting to the governing board about online safety.

ICT technicians are responsible for:

- Providing technical support in the development and implementation of the school's online safety policies and procedures.
- Implementing appropriate security measures as directed by the headteacher.
- Ensuring that the school's filtering and monitoring systems are updated as appropriate.

All staff members 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.
- Reporting concerns in line with the school's reporting procedure.
- Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum.

Pupils are responsible for:

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

3. [Updated] Managing online safety

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

The DSL has overall responsibility for the school's approach to online safety, with support from deputies and the 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.

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

- 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
- School participates in Safer Internet Day annually.

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.

[New] Staff will be aware that pupils may not feel ready or know how to tell someone about abuse they are experiencing, due to feeling embarrassed, humiliated, or threatened. Staff will be aware and recognise the importance of the presence and scale of online abuse or harassment, by considering that just because it is not being reported, does not mean it is not happening.

[New] 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.

[New] 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.

[New] 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 and appropriate support provided to the victim.

Concerns regarding a staff member's online behaviour are reported to the headteacher, who decides on the best course of action in line with the relevant policies, e.g. the Staff Code of Conduct, Allegations of Abuse Against Staff Policy, and Disciplinary Policy and Procedures. If the concern is about the headteacher, it is reported to the chair of governors.

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

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

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

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

4. [Updated] Cyberbullying

[Updated] 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
- **[New]** Abuse between young people in intimate relationships online i.e. teenage relationship abuse
- **[New]** Discriminatory bullying online i.e. homophobia, racism, misogyny/misandry.

[New] 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.

5. [Updated] 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.

[Updated] 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
- **[New]** Abuse between young people in intimate relationships online, i.e. teenage relationship abuse

[New] 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.

[New] 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 Child-on-child Abuse Policy and the Social Media Policy.

[Updated] The school responds 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 are reported to the DSL, who will investigate the matter in line with the Child-on-child Abuse Policy and the Child Protection and Safeguarding Policy.

6. Grooming and exploitation

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

Staff will be aware that grooming often takes place online and that pupils who are being groomed are commonly unlikely to report this behaviour for many reasons, including the following:

- The pupil believes they are talking to another child, when they are actually talking to an adult masquerading as someone younger with the intention of gaining their trust to abuse them.
- The pupil does not want to admit to talking to someone they met on the internet for fear of judgement, feeling embarrassed, or a lack of understanding from their peers or adults in their life.
- The pupil may have been manipulated into feeling a sense of dependency on their groomer due to the groomer’s attempts to isolate them from friends and family.
- Talking to someone secretly over the internet may make the pupil feel ‘special’, particularly if the person they are talking to is older.

- 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.
- 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 Policy. Staff will be expected to exercise vigilance towards any pupils displaying indicators that they have been, or are being, radicalised.

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

7. Mental health

The internet, particularly social media, can be the root cause of a number of mental health issues in pupils, e.g. low self-esteem and suicidal ideation.

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

8. Online hoaxes and harmful online challenges

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

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

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

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

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

- In line with any advice received from a known, reliable source, e.g. the UK Safer Internet Centre, when fact-checking the risk of online challenges or hoaxes.
- Careful to avoid needlessly scaring or distressing pupils.
- Not inadvertently encouraging pupils to view the hoax or challenge where they would not have otherwise come across it, e.g. where 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, e.g. it encourages children to participate in age-inappropriate activities that could increase safeguarding risks or become a child protection concern, 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 even to individual children at risk where appropriate.

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

9. Cyber-crime

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

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

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

The DSL and headteacher will ensure that pupils are taught, throughout the curriculum, how to use technology safely, responsibly and lawfully, and will ensure that pupils cannot access sites or areas of the internet that may encourage them to stray from lawful use of technology, e.g. the 'dark web', on school-owned devices or on school networks through the use of appropriate firewalls.

10. [Updated] Online safety training for staff

The DSL ensures that all safeguarding training given to staff includes elements of online safety, including how the internet can facilitate abuse and exploitation. 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.

[Updated] Information about the school's full responses to online safeguarding incidents can be found in the Anti-bullying Policy, the Child-on-child Abuse Policy and the Child Protection and Safeguarding Policy.

11. Online safety and the curriculum

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

- RSE
- Health education
- Wellbeing
- Citizenship
- Computing

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
- What healthy and respectful relationships, including friendships, look like
- Body confidence and self-esteem
- Consent, e.g. with relation to the sharing of indecent imagery or online coercion to perform sexual acts
- Acceptable and unacceptable online behaviour
- How to identify online risks
- How and when to seek support
- How to identify when something is deliberately deceitful or harmful
- How to recognise when something they are being asked to do puts them at risk or is age-inappropriate

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 A of this policy.

The school recognises that, while any pupil can be vulnerable online, there are some pupils who may be more susceptible to online harm or have less support from family and friends in staying safe online, e.g. pupils with SEND and LAC. Relevant members of staff, e.g. the SENCO and designated teacher for LAC, work together to ensure the curriculum is tailored so these pupils 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 review external resources prior to using them for the online safety curriculum, to ensure they are appropriate for the cohort of pupils. When reviewing these resources, the following questions are asked:

- Where does this organisation get their information from?

- What is their evidence base?
- Have they been externally quality assured?
- What is their background?
- Are they age-appropriate for pupils?
- Are they appropriate for pupils' developmental stage?

External visitors may be invited into school to help with the delivery of certain aspects of the online safety curriculum. The headteacher and DSL 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 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 advises the staff member on how to best support any pupil who may be especially impacted by a lesson or activity. Lessons and activities are 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 ensures 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.

12. Use of technology in the classroom

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

- Computers
- Laptops
- Tablets
- Internet
- 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 always reviews and evaluates the resource. Class teachers ensure that any internet-derived materials are used in line with copyright law.

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

13. Use of smart technology

While the school recognises that the use of smart technology can have educational benefits, there are also a variety of associated risks which 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 policies.

Staff will use all smart technology and personal technology in line with the school's policies.

The use of mobile phones on site for pupils is forbidden and mobile phones are handed in to teachers at the start of the day and returned at the end.

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.

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

14. Educating parents

The school works in partnership with parents to ensure pupils stay safe online at school and at home. Parents are provided with information about the school's approach to online safety and their role in protecting their children. Parents are encouraged to visit the school website regarding online safety where policies can be found.

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 is raised in the following ways:

- School website.
- Online resources

15. Internet access

Pupils, staff and other members of the school community are expected to follow the school policies when using the internet at school. Personal devices are not permitted access to the school network.

16. Filtering and monitoring online activity

The governing board ensures the school's ICT network has appropriate filters and monitoring systems in place. The governing board ensures 'over blocking' does not lead to unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.

The headteacher and ICT technicians undertake a risk assessment to determine what filtering and monitoring systems are required. The filtering and monitoring systems the school implements are 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 undertake checks on the filtering and monitoring systems to ensure they are effective and appropriate.

Requests regarding making changes to the filtering system are directed to the headteacher. Prior to making any changes to the filtering system, ICT technicians and the DSL conduct a risk assessment. Any changes made to the system are recorded by ICT technicians. Reports of inappropriate websites or materials are made to an ICT technician immediately, who investigates the matter and makes any necessary changes.

Deliberate breaches of the filtering system are 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. 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 are appropriately monitored. All users of the network and school-owned devices are informed about how and why they are monitored. Concerns identified through monitoring are reported to the DSL who manages the situation in line with the Child Protection and Safeguarding Policy.

17. Network security

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

Staff and pupils are advised not to open unfamiliar email attachments, and are expected to report all malware and virus attacks to ICT technicians.

All members of staff have their own unique usernames and private passwords to access the school's systems. Pupils in Y3 – Y6 and are provided with their own unique username and private passwords. Staff members and pupils are responsible for keeping their passwords private. Passwords have a minimum and maximum length and require a mixture of letters, numbers and symbols to ensure they are as secure as possible.

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

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

Full details of the school's network security measures can be found in the Data and Cyber-security Breach Prevention and Management Plan.

18. Emails

Access to and the use of emails is 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 are given approved school email accounts and are only 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.

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

Any cyber-attacks initiated through emails are managed in line with the Data and Cyber-security Breach Prevention and Management Plan.

19. Social networking

Personal use

Access to social networking sites is filtered as appropriate. Staff are not permitted to use social media for personal use during lesson time. Staff can use personal social media during break

and lunchtimes in designated areas; however, inappropriate or excessive use of personal social media during school hours may result in the removal of internet access or further action. Staff members are advised that their conduct on social media can have an impact on their role and reputation within the school. The Staff Code of Conduct contains information on the acceptable use of social media – staff members are required to follow these expectations at all times.

Staff are only permitted to communicate with pupils or parents over social networking sites where an existing relationship exists and then with due care and will ensure that their social media conduct relating to that parent is appropriate for their position in the school.

Concerns regarding the online conduct of any member of the school community on social media are reported to the DSL and managed in accordance with the relevant policy, e.g. Anti-Bullying Policy, Staff Code of Conduct and Behaviour Policy.

Use on behalf of the school

The use of social media on behalf of the school is conducted in line with the Social Media Policy. The school's official social media channels are only used for official educational or engagement purposes. Staff members must be authorised by the headteacher to access to the school's social media accounts.

All communication on official social media channels by staff on behalf of the school is clear, transparent and open to scrutiny.

20. The school website

The headteacher is 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 complies with guidelines for publications including accessibility, data protection, respect for intellectual property rights, privacy policies and copyright law. Personal information relating to staff and pupils is not published on the website. Images and videos are only posted on the website if the provisions in the Photography Policy are met.

21. Use of devices

School-owned devices

Staff members are issued with the following devices to assist with their work:

- Laptop
- Tablet

Pupils are provided with school-owned devices as necessary to assist in the delivery of the curriculum, e.g. tablets to use during lessons.

School-owned devices are used in accordance with the Device User Agreement. Staff and pupils are not permitted to connect school-owned devices to public Wi-Fi networks. All school-owned devices are password protected. All mobile school-owned devices are fitted with tracking software to ensure they can be retrieved if lost or stolen. All school-owned devices

are fitted with software to ensure they can be remotely accessed, in case data on the device needs to be protected, retrieved or erased.

ICT technicians review all school-owned devices on an ongoing basis to carry out software updates and ensure there is no inappropriate material or malware on the devices. No software, apps or other programmes can be downloaded onto a device without authorisation from ICT technicians.

Cases of staff members or pupils found to be misusing school-owned devices will be managed in line with the Disciplinary Policy and Procedure and Behaviour Policy respectively.

Personal devices

Personal devices are used in accordance with the Staff ICT and Electronic Devices Policy and the Pupils' Personal Electronic Devices Policy. Any personal electronic device that is brought into school is the responsibility of the user.

- Personal devices can only be used in public areas of school and the staff room – as highlighted in the staff handbook.

Staff members are not permitted to use their personal devices during lesson time, other than in an emergency. Staff members are not permitted to use their personal devices to take photos or videos of pupils.

Staff members report concerns about their colleagues' use of personal devices on the school premises in line with the Allegations of Abuse Against Staff Policy. If a member of staff is thought to have illegal content saved or stored on a personal device, or to have committed an offence using a personal device, the headteacher will inform the police and action will be taken in line with the Allegations of Abuse Against Staff Policy.

Where a pupil uses accessibility features on a personal device to help them access education, e.g. where a pupil who is deaf uses their mobile phone to adjust the settings on an internal hearing aid in response to audible stimuli during class, the arrangements and rules for conduct for this are developed and managed on a case-by-case basis.

Pupils' devices can be searched, screened and confiscated in accordance with the Searching, Screening and Confiscation Policy. If a staff member reasonably believes a pupil's personal device has been used to commit an offence or may provide evidence relating to an offence, the device will be handed to the police.

Appropriate signage is displayed to inform visitors to the school of the expected use of personal devices. Any concerns about visitors' use of personal devices on the school premises are reported to the DSL.

22. Remote learning

All remote learning is delivered in line with the school's Pupil Remote Learning Policy.

The school will risk assess the technology used for remote learning prior to use and ensure that there are no privacy issues or scope for inappropriate use. The school will consult with

parents prior to the period of remote learning about what methods of delivering remote teaching are most suitable – alternate arrangements will be made where necessary.

The school will ensure that all school-owned equipment and technology used for remote learning has suitable anti-virus software installed, can establish secure connections, can recover lost work, and allows for audio and visual material to be recorded or downloaded, where required.

During the period of remote learning, the school will maintain regular contact with parents to:

- Reinforce the importance of children staying safe online.
- Ensure parents are aware of what their children are being asked to do, e.g. sites they have been asked to use and staff they will interact with.
- Encourage them to set age-appropriate parental controls on devices and internet filters to block malicious websites.
- Direct parents to useful resources to help them keep their children safe online.

The school will not be responsible for providing access to the internet off the school premises and will not be responsible for providing online safety software, e.g. anti-virus software, on devices not owned by the school.

23. Monitoring and review

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

The next scheduled review date for this policy is October 2023.

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

Online harms and risks – curriculum coverage

Subject area	Description and teaching content	Curriculum area the harm or risk is covered in
How to navigate the internet and manage information		
Age restrictions	Some online activities have age restrictions because they include content which is not appropriate for children under a specific age. Teaching includes the following: • That age verification exists and why some online platforms ask users to verify their age • Why age restrictions exist • That content that requires age verification can be damaging to under-age consumers • What the age of digital consent is (13 for most platforms) and why it is important	This risk or harm is covered in the following curriculum areas: • Health education • Computing
How content can be used and shared	Knowing what happens to information, comments or images that are put online. Teaching includes the following: • What a digital footprint is, how it develops and how it can affect pupils' futures • How cookies work • How content can be shared, tagged and traced • How difficult it is to remove something once it has been shared online • What is illegal online, e.g. youth-produced sexual imagery (sexting)	This risk or harm is covered in the following curriculum areas: • **[Primary schools]** Relationships education • **[Secondary schools]** RSHE • Computing
Disinformation, misinformation and hoaxes	Some information shared online is accidentally or intentionally wrong, misleading or exaggerated. Teaching includes the following: • Disinformation and why individuals or groups choose to share false information in order to deliberately deceive • Misinformation and being aware that false and misleading information can be shared inadvertently • Online hoaxes, which can be deliberately and inadvertently spread for a variety of reasons	This risk or harm is covered in the following curriculum areas: • **[Primary schools]** Relationships and health education

	• That the widespread nature of this sort of content can often appear to be a stamp of authenticity, making it important to evaluate what is seen online • How to measure and check authenticity online • The potential consequences of sharing information that may not be true	• **[Secondary schools]** RSHE • **[KS2 and above]** Computing • **[KS3 and KS4]** Citizenship
Fake websites and scam emails	Fake websites and scam emails are used to extort data, money, images and other things that can either be used by the scammer to harm the person targeted or sold on for financial, or other, gain. Teaching includes the following: • How to recognise fake URLs and websites • What secure markings on websites are and how to assess the sources of emails • The risks of entering information to a website which is not secure • What pupils should do if they are harmed, targeted, or groomed as a result of interacting with a fake website or scam email • Who pupils should go to for support	This risk or harm is covered in the following curriculum areas: • **[Primary schools]** Relationships education • **[Secondary schools]** RSHE • Computing
Online fraud	Fraud can take place online and can have serious consequences for individuals and organisations. Teaching includes the following: • What identity fraud, scams and phishing are • That children are sometimes targeted to access adults' data • What 'good' companies will and will not do when it comes to personal details	This risk or harm is covered in the following curriculum areas: • **[Primary schools]** Relationships education • **[Secondary schools]** RSHE • Computing
Password phishing	Password phishing is the process by which people try to find out individuals' passwords so they can access protected content. Teaching includes the following:	This risk or harm is covered in the following curriculum areas: • **[Primary schools]**

	• Why passwords are important, how to keep them safe and that others might try to get people to reveal them • How to recognise phishing scams • The importance of online security to protect against viruses that are designed to gain access to password information • What to do when a password is compromised or thought to be compromised	Relationships education • **[Secondary schools]** RSHE • Computing
Personal data	Online platforms and search engines gather personal data – this is often referred to as 'harvesting' or 'farming'. Teaching includes the following: • How cookies work • How data is farmed from sources which look neutral • How and why personal data is shared by online companies • How pupils can protect themselves and that acting quickly is essential when something happens • The rights children have with regards to their data • How to limit the data companies can gather	This risk or harm is covered in the following curriculum areas: • **[Primary schools]** Relationships education • **[Secondary schools]** RSHE • Computing
Persuasive design	Many devices, apps and games are designed to keep users online for longer than they might have planned or desired. Teaching includes the following: • That the majority of games and platforms are designed to make money, and that their primary driver is to encourage people to stay online for as long as possible • How notifications are used to pull users back online	This risk or harm is covered in the following curriculum areas: • Health education • Computing
Privacy settings	Almost all devices, websites, apps and other online services come with privacy settings that can be used to control what is shared. Teaching includes the following: • How to find information about privacy settings on various devices and platforms • That privacy settings have limitations	This risk or harm is covered in the following curriculum areas: • **[Primary schools]**

		Relationships education • **[Secondary schools]** RSHE • Computing
Targeting of online content	Much of the information seen online is a result of some form of targeting. Teaching includes the following: • How adverts seen at the top of online searches and social media have often come from companies paying to be on there and different people will see different adverts • How the targeting is done • The concept of clickbait and how companies can use it to draw people to their sites and services	This risk or harm is covered in the following curriculum areas: • **[Primary schools]** Relationships education • **[Secondary schools]** RSHE • Computing
How to stay safe online		
Online abuse	Some online behaviours are abusive. They are negative in nature, potentially harmful and, in some cases, can be illegal. Teaching includes the following: • The types of online abuse, including sexual harassment, bullying, trolling and intimidation • When online abuse can become illegal • How to respond to online abuse and how to access support • How to respond when the abuse is anonymous • The potential implications of online abuse • What acceptable and unacceptable online behaviours look like	This risk or harm is covered in the following curriculum areas: • **[Primary schools]** Relationships education • **[Secondary schools]** RSHE • Computing • **[KS4]** Citizenship
Challenges	Online challenges acquire mass followings and encourage others to take part in what they suggest. Teaching includes the following: • What an online challenge is and that, while some will be fun and harmless, others may be dangerous and even illegal	This risk or harm is covered in the following curriculum areas: • **[Primary schools]**

	• How to assess if the challenge is safe or potentially harmful, including considering who has generated the challenge and why • That it is okay to say no and to not take part in a challenge • How and where to go for help • The importance of telling an adult about challenges which include threats or secrecy, such as 'chain letter' style challenges	Relationships education • **[Secondary schools]** RSHE
Content which incites violence	Knowing that violence can be incited online and escalate very quickly into offline violence. Teaching includes the following: • That online content (sometimes gang related) can glamorise the possession of weapons and drugs • That to intentionally encourage or assist in an offence is also a criminal offence • How and where to get help if they are worried about involvement in violence	This risk or harm is covered in the following curriculum areas: • **[Primary schools]** Relationships education • **[Secondary schools]** RSHE
Fake profiles	Not everyone online is who they say they are. Teaching includes the following: • That, in some cases, profiles may be people posing as someone they are not or may be 'bots' • How to look out for fake profiles	This risk or harm is covered in the following curriculum areas: • **[Primary schools]** Relationships education • **[Secondary schools]** RSHE • Computing
Grooming	Knowing about the different types of grooming and motivations for it, e.g. radicalisation, child sexual abuse and exploitation, and gangs and county lines. Teaching includes the following: • Boundaries in friendships with peers, in families, and with others • Key indicators of grooming behaviour	This risk or harm is covered in the following curriculum areas: • **[Primary schools]** Relationships education

	• The importance of disengaging from contact with suspected grooming and telling a trusted adult • How and where to report grooming both in school and to the police At all stages, it is important to balance teaching pupils about making sensible decisions to stay safe whilst being clear it is never the fault of the child who is abused and why victim blaming is always wrong.	• **[Secondary schools]** RSHE
Livestreaming	Livestreaming (showing a video of yourself in real-time online, either privately or to a public audience) can be popular with children, but it carries a risk when carrying out and watching it. Teaching includes the following: • What the risks of carrying out livestreaming are, e.g. the potential for people to record livestreams and share the content • The importance of thinking carefully about who the audience might be and if pupils would be comfortable with whatever they are streaming being shared widely • That online behaviours should mirror offline behaviours and that this should be considered when making a livestream • That pupils should not feel pressured to do something online that they would not do offline • Why people sometimes do and say things online that they would never consider appropriate offline • The risk of watching videos that are being livestreamed, e.g. there is no way of knowing what will be shown next • The risks of grooming	This risk or harm is covered in the following curriculum areas: • **[Secondary schools]** RSHE
Pornography	Knowing that sexually explicit material presents a distorted picture of sexual behaviours. Teaching includes the following: • That pornography is not an accurate portrayal of adult sexual relationships • That viewing pornography can lead to skewed beliefs about sex and, in some circumstances, can normalise violent sexual behaviour	This risk or harm is covered in the following curriculum areas: • **[Secondary schools]** RSHE

	• That not all people featured in pornographic material are doing so willingly, i.e. revenge porn or people trafficked into sex work	
Unsafe communication	Knowing different strategies for staying safe when communicating with others, especially people they do not know or have not met. Teaching includes the following: • That communicating safely online and protecting your privacy and data is important, regardless of who you are communicating with • How to identify indicators of risk and unsafe communications • The risks associated with giving out addresses, phone numbers or email addresses to people pupils do not know, or arranging to meet someone they have not met before • What online consent is and how to develop strategies to confidently say no to both friends and strangers online	This risk or harm is covered in the following curriculum areas: • **[Primary schools]** Relationships education • **[Secondary schools]** RSHE • Computing
Wellbeing		
Impact on confidence (including body confidence)	Knowing about the impact of comparisons to 'unrealistic' online images. Teaching includes the following: • The issue of using image filters and digital enhancement • The role of social media influencers, including that they are paid to influence the behaviour of their followers • The issue of photo manipulation, including why people do it and how to look out for it	This risk or harm is covered in the following curriculum areas: • **[Secondary schools]** RSHE
Impact on quality of life, physical and mental health and relationships	Knowing how to identify when online behaviours stop being fun and begin to create anxiety, including that there needs to be a balance between time spent online and offline. Teaching includes the following: • How to evaluate critically what pupils are doing online, why they are doing it and for how long (screen time) • How to consider quality vs. quantity of online activity	This risk or harm is covered in the following curriculum areas: • Health education

	• The need for pupils to consider if they are actually enjoying being online or just doing it out of habit, due to peer pressure or due to the fear or missing out • That time spent online gives users less time to do other activities, which can lead some users to become physically inactive • The impact that excessive social media usage can have on levels of anxiety, depression and other mental health issues • That isolation and loneliness can affect pupils and that it is very important for them to discuss their feelings with an adult and seek support • Where to get help	
Online vs. offline behaviours	People can often behave differently online to how they would act face to face. Teaching includes the following: • How and why people can often portray an exaggerated picture of their lives (especially online) and how that can lead to pressures around having perfect or curated lives • How and why people are unkind or hurtful online when they would not necessarily be unkind to someone face to face	This risk or harm is covered in the following curriculum areas: • **[Primary schools]** Relationships education • **[Secondary schools]** RSHE
Reputational damage	What users post can affect future career opportunities and relationships – both positively and negatively. Teaching includes the following: • Strategies for positive use • How to build a professional online profile	This risk or harm is covered in the following curriculum areas: • **[Secondary schools]** RSHE
Suicide, self-harm and eating disorders	Pupils may raise topics including eating disorders, self-harm and suicide. Teachers must be aware of the risks of encouraging or making these seem a more viable option for pupils and should take care to avoid giving instructions or methods and avoid using language, videos and images.	

Dore Primary School Pupil technology acceptable use agreement

At Dore Primary School, we know that it can be fun to use technology as part of your learning experience. We want everyone to be able to use technology, like computers and tablets, but it is important that you are safe when you are using them.

We have created this agreement to help you understand how to be safe when you are using technology. Please read this carefully and sign your name to show that you understand your responsibilities when using technology. Ask your teacher if there is something that you do not understand.



I will:

- ✓ Only use technology, such as a computer, when a teacher has given me permission.
- ✓ Only use technology for the reason I have been asked to use it.
- ✓ Only use the internet when a teacher has given me permission.
- ✓ Ask for help when I have a problem using the technology.
- ✓ Look after the device and try not to damage it.
- ✓ Tell the teacher if my device is not working or damaged.
- ✓ Tell the teacher if I think someone else is not using technology safely or correctly.
- ✓ Tell the teacher if I see something online that I think is inappropriate or that makes me upset.
- ✓ I will only use AI tools under the supervision and agreement of my teacher.

I will not:

- ✗ Tell another pupil my username and password.
- ✗ Share personal information, such as my age and where I live, about myself or my friends online.
- ✗ Access social media, such as Facebook and WhatsApp.
- ✗ Speak to strangers on the internet.

- ✘ Take photos of myself or my friends using a school device.

Technology acceptable use agreement for adults in school

Whilst our school promotes the use of technology, and understands the positive effects it can have on enhancing pupils' learning and community engagement, we must also ensure that adults use technology appropriately. Any misuse of technology will not be taken lightly and will be reported to the headteacher in order for any necessary further action to be taken.

This acceptable use agreement is designed to outline staff responsibilities when using technology, whether this is via personal devices or school devices, on or off the school premises, and applies to all staff, volunteers, contractors and visitors.

Please read this document carefully.

Using technology in school

- I will only use ICT systems which have been permitted for my use by the headteacher, such as:
  - Computers.
  - Laptops.
  - Tablets.
- I will only use the approved email accounts that have been provided to me.
- I will not use personal emails to send and receive personal data or information.
- I will not share sensitive personal data with any other staff, pupils or third parties unless explicit consent has been received.
- I will ensure that any personal data is stored in line with the UK GDPR.
- I will delete any chain letters, spam and other emails from unknown sources without opening them.
- I will only use the internet for personal use during out-of-school hours, including break and lunch times.
- I will not search for, view, download, upload or transmit any explicit or inappropriate material when using the internet.
- I will not share school-related passwords with pupils, staff or third parties unless permission has been given for me to do so.
- I will only use removeable media for non-sensitive data.
- I will only store sensitive personal data on staff share.

1. **Mobile devices**

- I will only use school-owned mobile devices for educational purposes.
- I will only use personal mobile devices during out-of-school hours, including break and lunch times and in the areas designated in the staff handbook.
- I will not use personal mobile devices to take photographs or videos of pupils or staff.
- I will not use mobile devices to send inappropriate messages, images or recordings.
- I will ensure that personal and school-owned mobile devices do not contain any inappropriate or illegal content.

- I will not access the WiFi system using personal mobile devices unless permission has been given by the headteacher.
- I will only use personal mobile devices to communicate with pupils or parents either in emergency or on school visits away from site.
- I will not store any images or videos of pupils, staff or parents on any mobile device unless consent has been sought from the individual(s) in the images or videos.
- In line with the above, I will only process images or videos of pupils, staff or parents for the activities for which consent has been sought.
-

2. Social media and online professionalism

- If I am representing the school online, e.g. through website, blogging or on a school social media account, I will express neutral opinions and will not disclose any confidential information regarding the school, or any information that may affect its reputability.
- I will not use any school-owned mobile devices to access personal social networking sites.
- I will not communicate with pupils or parents over personal social networking sites.
- I will not accept 'friend requests' or 'follow requests' from any current pupils or parents over personal social networking sites – unless a previous relationship was already established.
- I will ensure that I apply the necessary privacy settings to any social networking sites.
- I will not publish any comments or posts about the school on any social networking sites which may affect the school's reputability.
- I will not post or upload any defamatory, objectionable, copyright-infringing or private material, including images and videos of pupils, staff or parents, on any online website.
- I will not post or upload any images and videos of pupils, staff or parents on any online website without consent from the individual(s) in the images or videos.
- In line with the above, I will only post images or videos of pupils, staff or parents for the activities for which consent has been sought.
- I will not give my home address, phone number, mobile number, social networking details or email addresses to pupils or parents – any contact with parents will be done through authorised school contact channels.

3. Working from home

- I will adhere to the principles of the UK GDPR when working from home.
- I will ensure I obtain permission from the headteacher before any personal data is transferred from a school-owned device to a personal device.
- I will ensure any data transferred from a school-owned device to a personal device is encrypted or pseudonymised.
- I will ensure any sensitive personal data is not transferred to a personal device unless completely necessary – and, when doing so, that it is encrypted.
- I will ensure my personal device has been assessed for security by the online safety officer before it is used for lone working.

- I will ensure no unauthorised persons, such as family members or friends, access any personal devices used for lone-working.
- I will act in accordance with the school's Online Safety Policy when transporting school equipment and data.

4. Reporting misuse

- I will ensure that I adhere to any responsibility I have for monitoring, as outlined in the Online Safety Policy, e.g. to monitor pupils' internet usage.
- I will ensure that I report any misuse by pupils or staff members breaching the procedures outlined in this agreement to the headteacher.
- I understand that my use of the internet will be monitored by the online safety officer and SLT and recognise the consequences if I breach the terms of this agreement.
- I understand that the headteacher may decide to take disciplinary action against me, in accordance with the Disciplinary Policy and Procedure, if I breach this agreement.

Cyberbullying

1. Legal framework

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

- The Equality Act 2010
- The Safeguarding Vulnerable Groups Act 2006
- The Education and Inspections Act 2006
- The Computer Misuse Act 1990, amended by the Police and Justice Act 2006
- The Regulation of Investigatory Powers Act 2000
- **[Independent schools]** The Education (Independent School Standards) Regulations 2014
- The Education Act 2002
- The Criminal Justice and Courts Act 2015
- DfE (2017) 'Preventing and tackling bullying'
- DfE (2019) 'Keeping children safe in education'
- DfE (2018) 'Searching, screening and confiscation'

1.2. This policy operates in conjunction with the following school policies:

- **Acceptable Use Agreement (AUP)**
- **Online Safety Policy**
- **Anti-bullying Policy**
- **Child Protection and Safeguarding Policy**
- **Staff Handbook**

2. Roles and responsibilities

2.1. The **board of governors** is responsible for:

- The overall implementation and monitoring of this policy.
- Appointing a safeguarding link governor who will work with the **DSL** to ensure the policies and practices relating to safeguarding, including the prevention of cyberbullying, are being implemented effectively.

2.2. The **headteacher** is responsible for:

- The practices and procedures outlined in this policy and ensuring that their effectiveness is monitored.
- Ensuring that the school maintains details of agencies and resources that may assist in preventing and addressing cyberbullying.
- Reviewing the procedures outlined in the school's **Online Safety Policy** to ensure that pupils protect themselves from cyberbullying online.
- Ensuring all incidents of cyberbullying are reported and dealt with in accordance with the school's **Anti-bullying Policy**.

2.3. The **DSL** is responsible for:

- Ensuring all policies that relate to safeguarding, including cyberbullying, are reviewed and updated regularly.
- Ensuring all staff are aware that they must report any issues concerning cyberbullying and know how to do so.
- Providing training to all staff so that they feel confident identifying pupils at risk of being cyberbullied and know how to make referrals when a pupil is at risk.
- Ensuring that parents are provided access to this policy so that they are fully aware of the school's responsibility to safeguard pupils and their welfare.
- Ensuring all pupils are taught about cyberbullying and how they should report a concern.
- Ensuring all staff are aware of their responsibilities by providing clear guidance for staff on the use of technology, both inside and outside of school.

2.4. All members of staff are responsible for identifying signs of cyberbullying and staying informed about the technologies that pupils commonly use.

2.5. **Teachers** are responsible for ensuring that issues surrounding cyberbullying are explored in the curriculum and pupils are aware of how to respect others.

2.6. Pupils, staff and parents are responsible for complying with the school's **Acceptable Use Agreement**. Pupils will be asked to sign the agreement before they are allowed to use computer equipment and the internet in school. Parents will be asked to confirm that they have discussed its contents with their children.

3. What is cyberbullying?

3.1. For the purpose of this policy, "**bullying**" is an act which is based on unequal power relations, real or perceived. It will usually be repeated and be difficult to defend against and is intended to hurt the recipient emotionally and/or physically. It can manifest verbally, in writing or images, and can be done physically, financially (including damage to property) or through social isolation. Verbal bullying is the most common form, especially within schools.

3.2. For the purpose of this policy, "**cyberbullying**" includes sending or posting harmful or upsetting text, images or other messages using the internet, mobile phones or other ICT for the purpose of bullying.

3.3. Cyberbullying can take many forms and can go even further than face-to-face bullying by invading personal space and home life, and can target more than one person. It can also take place across age groups and target pupils, staff and others, and may take place inside school, within the wider community, at home or when travelling. It can sometimes draw bystanders into being accessories.

3.4. Cyberbullying can include the following:

- Threatening, intimidating or upsetting text messages
- Threatening or embarrassing pictures and video clips sent via mobile phone cameras
- Disclosure of private sexual photographs or videos with the intent to cause distress
- 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
- Menacing or upsetting responses to someone in a chatroom
- Unpleasant messages sent via instant messaging
- Unpleasant or defamatory information posted to blogs, personal websites and social networking sites, e.g. Facebook

NB. The above list is not exhaustive, and cyberbullying may take other forms.

3.5. All cases of cyberbullying are considered to be as serious as any other form of bullying.

3.6. Cyberbullying issues are dealt with in an appropriate manner dependent on the severity and frequency of the issue, in accordance with the school's **Anti-bullying Policy.**

4. Legal issues

4.1. Cyberbullying is generally criminal in character.

4.2. It is unlawful to disseminate defamatory information in any media, including via websites.

4.3. Section 127 of the Communications Act 2003 makes it an offence to send, by public means of a public electronic communications network, a message or other matter that is grossly offensive, or one of an indecent, obscene or menacing character.

4.4. In addition, the Protection from Harassment Act 1997 makes it an offence to knowingly pursue any course of conduct amounting to harassment.

4.5. At the school, cyberbullying is considered as serious as any other form of bullying. Cyberbullying issues are dealt with in an appropriate manner dependent on the severity and frequency of the issue and the age of the pupil.

5. Preventing cyberbullying

5.1. The school recognises that both staff and pupils may experience cyberbullying and will commit to preventing any instances that may occur by creating a learning and teaching environment which is free from harassment and bullying.

5.2. Staff, pupils and parents will be regularly educated about cyberbullying and the importance of staying safe online, in accordance with the school's **Online Safety Policy**.

5.3. Teachers will discuss cyberbullying as part of the curriculum, and diversity, difference and respect for others will be promoted and celebrated through various lessons.

5.4. Pupils will be educated about the importance of reporting instances of cyberbullying and will be fully informed of who they should report any concerns to.

5.5. Staff will be regularly educated about the signs of cyberbullying in order to promote early identification and intervention.

5.6. It is made clear in staff meetings and the staff handbook that members of staff should not have contact with current pupils on social networking sites (specifically, not befriending pupils on Facebook). In addition, staff are discouraged from having past pupils as friends.

5.7. The delivery of PSHE is important and will include discussing keeping personal information safe and the appropriate use of the internet. In addition, pupils will be educated about online safety through projects in other subjects, such as computing.

5.8. Outside the curriculum, pupils will receive regular pastoral sessions about e-safety and cyberbullying through assemblies, conferences and Anti-Bullying Week.

5.9. Pupils will have a voice through the student council to ensure they are fully engaged and involved in evaluating and improving policy and procedures.

6. Signs of being cyberbullied

6.1. All members of staff will receive training on a **regular** basis on the signs of cyberbullying, in order to identify pupils who may be experiencing issues and intervene effectively.

6.2. Staff will be alert to the following signs that may indicate a pupil is being cyberbullied:

- Becoming withdrawn or shy
- Showing signs of depression
- Becoming extremely moody or agitated
- Becoming anxious or overly stressed
- Displaying signs of aggressive behaviour
- Avoiding use of the computer
- Changing eating and/or sleeping habits
- Avoiding participating in activities they once enjoyed
- Engaging in self-harm, or threatening/attempting suicide
- Changing their group of friends suddenly

6.3. Staff will also be alert to the following signs which may indicate that a pupil is cyberbullying others:

- Avoiding using the computer or turning off the screen when someone is near
- Appearing nervous when using the computer or mobile phone
- Acting in a secretive manner when using the computer or mobile phone
- Spending excessive amounts of time on the computer or mobile phone
- Becoming upset or angry when the computer or mobile phone is taken away

7. Procedures for dealing with cyberbullying

7.1. All issues of cyberbullying should be reported according to the procedures outlined in the **Anti-bullying Policy**.

7.2. If staff are concerned that a pupil might be at risk of cyberbullying, they will report this to the **DSL** as soon as possible.

7.3. All pupils will be informed that they can disclose cyberbullying concerns about themselves or others to any member of staff. Staff will not promise confidentiality and will inform the **DSL** of the disclosure as soon as possible.

7.4. Responses to cyberbullying incidents, including the necessary sanctions, will be dealt with in accordance with the school's **Anti-bullying Policy**.

7.5. A cyberbullying incident might include features different to other forms of bullying, prompting a particular response. Significant differences may include the following:

- **Impact**: possible extensive scale and scope
- **Location**: the anytime and anywhere nature of cyberbullying
- **Anonymity**: the person being bullied might not know who the perpetrator is
- **Motivation**: the perpetrator might not realise that their actions are bullying
- **Evidence**: the subject of the bullying may have evidence of what has happened

7.6. Any cyberbullying incidents that involve members of staff will be dealt with in accordance with the school's **disciplinary procedures.**

7.7. Staff are required to report any concerns to the **headteacher**, who will investigate the matter and will initiate an appropriate response.

7.8. All incidents of cyberbullying, including any concerns, will be recorded and securely held on CPOMs.

7.9. The **headteacher** will arrange a discussion with the victimised pupil in order to gain knowledge about the situation, and will use this to inform a discussion with the pupil who has been accused of cyberbullying.

7.10. The **headteacher** will discuss the incident with any witnesses and will gain evidence of the cyberbullying incident; this may involve text messages, emails, photos, etc., provided by the victim.

7.11. The school understands that pupils at primary level, and particularly younger children, may not be aware of their actions and, as such, may not mean to intentionally cyberbully another pupil.

7.12. The **headteacher** will take into account the nature of the cyberbullying incident and the way in which it has been conducted, including if it is evident that it was intentional or if the pupil's age and knowledge of cyberbullying is a contributing factor to the incident, when deciding on the appropriate sanction.

7.13. If necessary, the **headteacher** may decide to involve the police in an appropriate response to the cyberbullying incident.

7.14. If necessary, the **headteacher** will liaise with the **online safety co-ordinator** when issuing an appropriate sanction, such as by removing internet access, monitoring the pupil's internet use, etc., in accordance with the **Online Safety Policy**.

8. Support for the pupil being bullied

8.1. The **headteacher** will discuss the support available with the victim and, therefore, their feelings and requests are paramount to the support provided.

8.2. The support available includes:

- Emotional support and reassurance, if necessary arranged through external sources.
- Reassurance that it was right to report the incident and that appropriate action will be taken.
- Liaison with the pupil's parents to ensure a continuous dialogue of support.
- Advice not to retaliate or reply, but to keep the evidence and show or give it to their parent or a member of staff.
- Advice on other aspects of e-safety procedures to prevent re-occurrence.
- Discussion with the pupil's parents to evaluate their online habits.
- Age-appropriate advice on how the perpetrator might be blocked online.
- Actions, where possible and appropriate, to have offending material removed.
- Discussion with the pupil's parents on whether police action is required (except in serious cases of child exploitation where the police may be contacted without discussion with parents).

8.3. The school will also use additional support, such as involvement with external agencies, where necessary, as outlined in the **Anti-bullying Policy**.

9. Investigation and legal powers

9.1. The nature of any investigation will depend on the circumstances. It may include the following:

- Preserving evidence, for example, by saving or printing (e.g. phone messages, texts, emails and website pages)
- Efforts to identify the perpetrator, which may include looking at the media, systems and sites used; however, members of staff do not have the authority to search the contents of a phone unless the device has been seized in a lawful 'without consent' search and is prohibited by the school rules, or is suspected of being, or likely to be, used to commit an offence or cause personal injury or damage to property
- Identifying and questioning witnesses
- Contacting the CEOP centre if images might be illegal or raise child protection issues
- Requesting that a pupil reveals a message or other phone content or confiscating a phone
- Legal action, e.g. where private sexual videos or images of an individual under 16-years-old are disclosed with the intent to cause distress

10. Working with the perpetrator

10.1. How the school will work with the perpetrator and any sanctions given will be determined on an individual basis in accordance with the **Anti-Bullying Policy**, with the intention of:

- Helping the victim to feel safe again and be assured that the bullying will stop.
- Holding the perpetrator to account, so they recognise the harm caused and do not repeat the behaviour.
- Helping bullies to recognise the consequences of their actions and facilitating change in their attitude and behaviour.
- Demonstrating that cyberbullying, as with any other form of bullying, is unacceptable, and that the school has effective ways of dealing with it.

11. Monitoring and review

11.1. This policy will be reviewed on an **annual** basis and changes necessary will be made, taking into account previous cyberbullying incidents and the effectiveness of procedures, and will communicate changes to all members of staff.

11.2. All members of staff are required to familiarise themselves with this policy as part of their induction programme.

Acceptable use of AI

Contents:

Statement of intent

At Dore Primary School, we recognise that the use of artificial intelligence (AI) can help to positively affect teacher workload, develop pupils' intellectual capabilities and prepare them for how emerging technologies will change workplaces. While there are many benefits to the use of AI tools, the content they produce may not always be accurate, safe or appropriate, and could lead to malpractice.

Through the measures outlined in this policy, the school aims to ensure that AI is used effectively, safely and appropriately to deliver excellent education that prepares our pupils to contribute to society and the future workplace.

For the purposes of this policy, the following terms are defined as:

- **AI** – The theory and development of computer systems able to perform tasks normally requiring human intelligence, e.g. visual perception, speech recognition, decision-making.
- **Generative AI** – A category of AI algorithms that generate new outputs based on the data they have been trained on.
- **Misuse of AI** – Any use of AI which means that pupils have not independently demonstrated their own attainment.

1. Legal framework

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

- Data Protection Act 2018
- The UK General Data Protection Regulation (UK GDPR)
- DfE (2022) 'Keeping children safe in education 2022'
- DfE (2023) 'Generative artificial intelligence in education'
- DfE (2023) 'Meeting digital and technology standards in schools and colleges'
- JCQ (2023) 'Artificial Intelligence (AI) Use in Assessments: Protecting the Integrity of Qualifications'
- JCQ (2023) 'Suspected Malpractice Policies and Procedures'

This policy operates in conjunction with the following school policies:

- Online Safety Policy
- Cyber-security Policy
- Cyber Response and Recovery Plan
- Data Protection Policy
- Child Protection and Safeguarding Policy
- Acceptable Use Agreement

2. Roles and responsibilities

The governing board will be responsible for:

- Ensuring that this policy is effective and complies with relevant laws and statutory guidance.
- Reviewing this policy on an annual basis.
- Ensuring their own knowledge of the use of AI tools in the school is up-to-date.
- Ensuring all staff undergo child protection and safeguarding training, including online safety, at induction and at regular intervals.
- Ensuring the school follows the DfE's digital and technology standards.

The headteacher will be responsible for:

- Ensuring that staff receive regular, up-to-date training on how to use AI tools in school.
- Ensuring that the use of AI tools in the school is integrated into relevant policies and procedures, the curriculum and staff training.
- Communicating with parents to ensure they are kept up-to-date with how AI tools are being used in the school, how this will impact pupils' education and how the school is ensuring the tools are being used safely and effectively.
- Working with the governing board to review and update this policy on an annual basis.
- Ensuring that AI practices are audited and evaluated on a regular basis.

ICT technicians will be responsible for:

- Providing technical support in the development and implementation of the school's AI practices, policies and procedures.
- Implementing appropriate security measures.
- Ensuring that the use of AI tools is taken into consideration when creating policies and procedures regarding online safety, child protection and safeguarding, and data protection.

The DPO will be responsible for:

- Keeping up-to-date and informed with AI technologies relevant to the school.
- Understanding and maintaining awareness of what the use of AI means for data protection in the school.
- Advising the school on how to integrate the use of AI while complying with data protection regulations.

The DSL will be responsible for:

- Taking the lead responsibility for online safety in school.
- Undertaking training so they understand the risks associated with using AI tools in school.
- Liaising with relevant members of staff on online safety matters.
- Maintaining records of reported online safety concerns relating to the use of AI tools, as well as the actions taken in response to concerns.
- Reporting to the governing board about the use of AI tools and how it links to safeguarding.

All staff members will be responsible for:

- Adhering to the Acceptable Use Agreement and other relevant policies.
- Taking responsibility for the security of the AI tools and data they use or have access to.
- Modelling good online behaviours when using AI tools.
- Maintaining a professional level of conduct in their use of AI tools.
- Having an awareness of the risks that using AI tools in school poses.
- Reporting concerns in line with the school's reporting procedure.
- Where relevant to their role, ensuring that the safe and effective use of AI tools is embedded in their teaching of the curriculum.
- Familiarising themselves with any AI tools used by the school and the risks they pose.

Pupils will be responsible for:

- Adhering to the Acceptable Use Agreement and other relevant policies.
- Seeking help from the relevant school staff if they are concerned about an experience that they or a peer has experienced while using AI tools.
- Reporting concerns in line with the school's reporting procedure.
- Familiarising themselves with any AI tools used by the school and the risks they pose.

3. Data protection and cyber-security

The school is aware of the data privacy and cyber-security implications that come with using generative AI tools, and will ensure that all AI tools are used in line with the school's Data Protection Policy and Cyber-security Policy. The school will follow the procedures in these policies to continue to protect pupils from harmful online content that could be produced by AI tools.

The school will not enter data that is classed as personal and sensitive into AI tools under any circumstances. Any data entered will not be identifiable, and will be considered released to the internet.

All staff will be made aware that generative AI tools are able to create believable content of all kinds, for example credible email scams requesting payment, and that the content AI produces may seem more authoritative and believable than usual scams. All staff will apply their best judgement and common sense to manage cyber-security risks effectively and ensure that the DfE's cyber standards are followed at all times.

4. Using AI tools

The school will ensure that AI tools are used appropriately to achieve the following aims:

- To reduce workload
- To free up teachers' time
- To produce high-quality and compliant administrative plans, policies and documents
- To support the teaching of a knowledge-rich computing curriculum
- To teach pupils:
    - How to use emerging technologies safely and appropriately.
    - About the limitations, reliability and potential bias of AI tools.
    - How information on the internet is organised and ranked.
    - How online safety practices can protect against harmful and misleading content.
    - To identify and use appropriate resources to support their education, including age-appropriate resources and preventing over-reliance on a limited number of tools or resources.

Where AI tools are used to produce administrative plans, policies and documents, all staff members will understand that the quality and content of the final document remains the professional responsibility of the staff member who produced it. Staff members using AI tools to create documents will not assume that AI output will be comparable with a human-designed document that has been developed in the specific context of the school.

Pupils will be made aware of the importance of referencing AI tools correctly when using AI tools to produce work, especially if the work is for an assessment, in order to allow teachers and assessors to review how AI has been used and whether it was appropriate. Pupils' references to AI sources will show the name of the AI source and the date that the content was generated.

Pupils will retain a copy of the questions and AI generated content for reference and authentication purposes in a non-editable format, e.g. a screenshot. Pupils will also provide a brief explanation of how AI tools have been used.

5. Misusing AI tools

Preventing misuse

The school acknowledges that misuse of AI tools can happen both accidentally and intentionally, and that education and awareness is key to preventing misuse. The school will consider taking the following actions to prevent the misuse of AI tools:

- Restricting access to online AI tools on school devices and networks, especially on devices used for exams and assessments
- Setting reasonable deadlines for submission of work and providing pupils with regular reminders
- Allocating time for sufficient portions of pupils' work to be completed in class under direct supervision, where appropriate
- Examining intermediate stages in the production of pupils' work to ensure that work is being completed in a planned and timely manner, and that work submitted represents a natural continuation of earlier stages
- Introducing classroom activities that use the level of knowledge and understanding achieved during lessons to ensure the teacher is confident that pupils understand the material
- Engaging pupils in verbal discussions about their work to ascertain that they understand it and that it reflects their own independent work
- Refusing to accept work that is suspected to have been generated through misuse of AI tools without further investigation
- Issuing tasks which are, wherever possible, topical, current and specific, and require the creation of content which is less likely to be accessible to AI models
- Investing in educating and training staff, pupils and parents on the use of AI tools and raising awareness of the risks and issues that come with its use

Identifying misuse

Staff members will continue to use the skills and observation techniques already in use to assure themselves that pupils' work is authentically their own when attempting to identify a misuse of AI tools.

When reviewing pupils' work to ensure its authenticity, staff members will compare it against other work created by the pupil. Where the work is made up by writing, the staff members will make note of:

- Spelling and punctuation.
- Grammatical usage.
- Writing style and tone.
- Vocabulary.
- Complexity and coherency.
- General understanding and working level.

- The mode of production, i.e. whether the work was handwritten or word-processed.

Staff members will be aware of and look out for potential indicators of AI use, which include:

- A default use of American spelling, currency, terms and other localisations.
- A default use of language or vocabulary which might not appropriate to the working or qualification level.
- A lack of direct quotations and/or use of references where these are required or expected.
- Inclusion of references which cannot be found or verified.
- A lack of reference to events occurring after a certain date, reflecting when an AI tool's data source was compiled.
- Instances of incorrect or inconsistent use of first-person and third-person perspective where AI generated text has been left unaltered.
- A variation in the style of language evidenced in a piece of work, if a pupil has taken specific portions of text from an AI tool and then amended it.
- A lack of graphs, data tables or visual aids where these would normally be expected.
- A lack of specific, local or topical knowledge.
- Content being more generic in nature.
- The inadvertent inclusion of warnings or provisos produced by AI tools to highlight the limits of its ability or the hypothetical nature of its output.
- The submission of pupil work in a typed format, where this is not usual, expected or required.
- The unusual use of several concluding statements throughout the text, or several repetitions of an overarching essay structure within a single lengthy essay.
- The inclusion of confidently incorrect statements within otherwise cohesive content.

Staff members will remain aware that AI tools can be instructed to employ different languages and levels of proficiency when generating content, and some are able to produce quotations and references.

Where necessary, the school will make use of the following programmes and services that are able to analyse content and determine the likelihood that it was produced by AI:

- OpenAI Classifer
- GPTZero
- The Giant Language Model Test Room (GLTR)

6. Safeguarding

The school acknowledges that generative AI tools can be used to produce content that is dangerous, harmful, and inappropriate. The school will follow the procedures set out in the Child Protection and Safeguarding Policy and the Online Safety Policy to ensure that pupils are not able to access or be exposed to harmful content.

Pupils will be taught about the risks of using AI tools and how to use them safely. Pupils will be made aware of how to report any concerns or incidents involving generative AI, and who to talk to about any issues regarding the use of AI tools.

The school will engage with parents to inform them of the safeguarding risks that come with using AI tools, and how the school is protecting pupils online. The school will ensure that parents are aware of who to speak to about any concerns or issues regarding the use of AI.

The school will ensure that the appropriate filtering and monitoring systems are in place to protect pupils online, following the DfE's filtering and monitoring standards.

7. Monitoring and review

The governing board and headteacher will review this policy in full on an annual basis, and following any incidents that occur due to the use of AI tools, e.g. data protection or cyber-security.

The next scheduled review date for this policy is June 2024

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