

Online Safety Policy

Revised: September 2025
To be revised: September 2028

Contents

Legal framework	2
Roles and responsibilities	3
Managing online safety.....	4
Cyberbullying	6
Child-on-child sexual abuse and harassment	6
Grooming and exploitation	7
Mental health.....	8
Online hoaxes and harmful online challenges	8
Cyber-crime.....	9
Online safety training for staff.....	10
Online safety and the curriculum	10
Use of technology in the classroom.....	12
Use of smart technology	13
Educating parents	14
Internet access.....	14
Filtering and monitoring online activity.....	14
Network security.....	15
Emails	16
Generative artificial intelligence (AI)	16
Social networking.....	17
The school website	17
Use of devices	17
Remote learning.....	17
Monitoring and review	17

Statement of intent

Ightham 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.

Legal framework

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

- Online Safety Act (2023)
- [Voyeurism \(Offences\) Act 2019](#)
- [The UK General Data Protection Regulation \(UK GDPR\)](#)
- [Data Protection Act 2018](#)
- DfE (2025) '[Filtering and monitoring standards for schools and colleges](#)'
- DfE (2021) '[Harmful online challenges and online hoaxes](#)'
- DfE (2025) '[Keeping children safe in education 2025](#)'
- DfE (2023) '[Teaching online safety in school](#)'
- DfE (2022) '[Searching, screening and confiscation](#)'
- DfE (2023) '[Generative artificial intelligence in education](#)'
- Department for Digital, Culture, Media and Sport and UK Council for Internet Safety (2020) '[Sharing nudes and semi-nudes: advice for education settings working with children and young people](#)'
- UK Council for Child Internet Safety (2020) '[Education for a Connected World – 2020 edition](#)'
- National Cyber Security Centre (2020) '[Small Business Guide: Cyber Security](#)'

This policy operates in conjunction with the following school policies:

- Allegations of Abuse Against Staff and Volunteers Policy
- Acceptable Use Agreement
- Cyber-security Policy
- Child Protection and Safeguarding Policy
- Staff Code of Conduct
- Behaviour and Anti-Bullying Policy
- Disciplinary Policy and Procedure
- Data Protection Policy
- Confidentiality Policy
- Photography and Images Policy
- Remote Education Policy

- Responsible AI Use Policy

Roles and responsibilities

The DPO 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 online safety issues is up-to-date

The headteacher will be responsible for:

- Ensuring the DSL's remit covers online safety.
- Ensuring all staff undergo safeguarding and child protection training, including online safety, at induction and at regular intervals.
- Ensuring that the effectiveness of filtering and monitoring systems is reviewed at least annually in liaison with ICT staff and service providers.
- Ensuring that the SLT and other relevant staff have an awareness and understanding of the filtering and monitoring provisions in place, and manage them effectively and know how to escalate concerns when identified.
- Ensuring that all relevant school policies have an effective approach to planning for, and responding to, online challenges and hoaxes embedded within them.
- 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.
- Ensuring compliance with the DfE's 'Meeting digital and technology standards in schools and colleges', with particular regard to the filtering and monitoring standards in relation to safeguarding.
- Appointing an SLT digital lead in line with the cyber security policy
- 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.
 - Organising engagement with parents to keep them up-to-date with current online safety issues and how the school is keeping pupils safe, such as the national college or Knowsley City Learning Centre.

The DSL will be responsible for:

- Taking the lead responsibility for online safety in the school.
- 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, Computing teacher 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 CPOMs is used for reporting online safety incidents and inappropriate internet use, both by pupils and staff, and ensuring all members of the school community understand this procedure.
- Understanding the filtering and monitoring processes in place at the school.
- Ensuring that all safeguarding training given to staff includes an understanding of the expectations, roles and responsibilities in relation to filtering and monitoring systems at the school.
- 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.

Head of IT will be responsible for:

- Ensuring that there are appropriate filtering and monitoring systems in place.
- 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 will be responsible for:

- Taking responsibility for the security of ICT systems and electronic data they use or have access to.
- Ensuring their used device's software is kept up to date.
- 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.
- Report any concerns of possible scams, hacks or malware on their device which may have come from a download or online use.
- Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum.

Pupils will be 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.

Managing online safety

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

The DSL 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.

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

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

Handling online safety concerns

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

Staff will be aware that harmful online sexual behaviour can progress on a continuum, and appropriate and early intervention can prevent abusive behaviour in the future. Staff will also acknowledge that pupils displaying this type of behaviour are often victims of abuse themselves and should be suitably supported.

The victim of online harmful sexual behaviour may ask for no one to be told about the abuse. The DSL will consider whether sharing details of the abuse would put the victim in a more harmful position, or whether it is necessary in order to protect them from further harm. Ultimately the DSL will balance the victim's wishes against their duty to protect the victim and other young people. The DSL and other appropriate staff members will meet with the victim's parents to discuss the safeguarding measures that are being put in place to support their child and how the report will progress.

Confidentiality will not be promised, and information may be still shared lawfully, for example, if the DSL decides that there is a legal basis under UK GDPR such as the public task basis whereby it is in the public interest to share the information. If the decision is made to report abuse to children's social care or the police against the victim's wishes, this must be handled extremely carefully – the reasons for sharing the information should be explained to the victim and appropriate specialised support should be offered.

Concerns regarding a staff member's online behaviour are reported to the headteacher, who decides on the best course of action in line with the relevant policies. 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.

Cyberbullying

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

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

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.

Child-on-child sexual abuse and harassment

Pupils may also use the internet and technology as a vehicle for sexual abuse and harassment. Staff will understand that this abuse can occur both in and outside of school, off and online, and will remain aware that pupils are less likely to report concerning online sexual behaviours, particularly if they are using websites that they know adults will consider to be inappropriate for their age.

The following are examples of online harmful sexual behaviour of which staff will be expected to be aware:

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

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

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

The school will be aware that interactions between the victim of online harmful sexual behaviour and the alleged perpetrator(s) are likely to occur over social media following the initial report, as well as interactions with other pupils taking “sides”, often leading to repeat harassment. The school will respond to these incidents in line with the Child-on-child Abuse Policy and the Social Media Policy.

The school will respond to all concerns regarding online child-on-child sexual abuse and harassment, regardless of whether the incident took place on the school premises or using school-owned equipment. Concerns regarding online child-on-child abuse will be reported to the DSL, who will investigate the matter in line with the Child-on-child Abuse Policy and the Child Protection and Safeguarding Policy.

Grooming and exploitation

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

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

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

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

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

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

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

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

Radicalisation

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

Staff members will be aware of the factors which can place certain pupils at increased vulnerability to radicalisation, as outlined in the Prevent Duty 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.

Mental health

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

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, they will ensure that the challenge is directly addressed to the relevant pupils, e.g. those within a particular age range that is directly affected or individual pupils at risk where appropriate.

The DSL and 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.

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.

Online safety training for staff

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

Staff training will include a specific focus on harmful online narratives such as misinformation, disinformation, and conspiracy theories, helping staff to recognise the signs of influence or vulnerability among pupils.

Training will equip staff with the knowledge and confidence to identify signs of online harm, respond appropriately to disclosures or concerns, and support pupils in developing critical thinking skills and safe online behaviours.

Staff will also be guided on how to embed online safety themes across the wider curriculum, promoting a consistent, whole-school approach to digital safeguarding

Online safety and the curriculum

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

- Relationships and health education
- PSHE
- ICT

Online safety teaching is always appropriate to pupils' ages and developmental stages.

Pupils are taught the underpinning knowledge and behaviours that can help them to navigate the online world safely and confidently regardless of the device, platform or app they are using. The underpinning knowledge and behaviours pupils learn through the curriculum include the following:

- How to evaluate what they see online
- How to recognise techniques used for persuasion
- Acceptable and unacceptable online behaviour
- How to identify online risks
- How and when to seek support

- Knowledge and behaviours that are covered in the government's online media literacy strategy

The online risks pupils may face online are always considered when developing the curriculum. The risks that are considered and how they are covered in the curriculum can be found in [appendix A](#) of this policy.

Online Safety is taught at the beginning of every half term, with a focus linking to National online concerns. The Kapow scheme of work is reviewed regularly, guaranteeing up-to-date information is shared with students, at an age appropriate level. The progression of the scheme, [appendix B](#), ensuring a foundation for subject knowledge is built on from an early age.

The school's approach to teaching online safety in the curriculum will reflect the ever-evolving nature of online risks, ensuring pupils develop the knowledge and resilience to navigate digital spaces safely and responsibly. Online safety education will address four key categories of risk: content, contact, conduct, and commerce.

Content Risks

Pupils will be taught how to critically evaluate online content and identify material that is illegal, inappropriate, or harmful. The curriculum will include discussions around harmful content such as pornography, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, extremism, misinformation, disinformation (including fake news), and conspiracy theories. Lessons will equip pupils with the skills to question sources, verify information, and understand the dangers of engaging with such content.

Contact Risks

The school will educate pupils about the potential dangers of interacting with others online. Pupils will explore topics such as peer pressure, commercial exploitation, and grooming tactics used by adults who pose as children or young adults. They will learn how to recognise unsafe interactions, use privacy settings effectively, and report any concerning behaviour or messages to trusted adults and platforms.

Conduct Risks

Pupils will be guided on how their own online behaviour can impact both themselves and others. The curriculum will address the risks associated with creating, sharing, or receiving explicit images, including both consensual and non-consensual exchanges of nudes and semi-nudes. Online bullying, including the use of social media and messaging platforms to harass or intimidate others, will also be a key focus. Pupils will be taught responsible digital conduct and the legal and emotional consequences of harmful behaviour.

Commerce Risks

The curriculum will also include education on online commercial risks. Pupils will be informed about the dangers of online gambling, exposure to inappropriate advertising, and financial scams such as phishing. They will learn how to recognise fraudulent schemes, protect their personal and financial information, and seek help when confronted with suspicious online activity.

The DSL will be involved with the development of the school's online safety curriculum. Pupils will be consulted on the online safety curriculum, where appropriate, due to their unique knowledge of the kinds of websites they and their peers frequent and the kinds of behaviours in which they engage online.

Relevant members of staff, e.g. the SENCO and designated teacher for LAC, will work together to ensure the curriculum is tailored so that pupils who may be more vulnerable to online harms, e.g. pupils with SEND and LAC, receive the information and support they need.

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

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

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

Before conducting a lesson or activity on online safety, the class teacher and DSL will consider the topic that is being covered and the potential that pupils in the class have suffered or may be suffering from online abuse or harm in this way. The DSL will advise the staff member on how to best support any pupil who may be especially impacted by a lesson or activity. Lessons and activities will be planned carefully so they do not draw attention to a pupil who is being or has been abused or harmed online, to avoid publicising the abuse.

During an online safety lesson or activity, the class teacher will ensure a safe environment is maintained in which pupils feel comfortable to say what they feel and ask questions, and are not worried about getting into trouble or being judged.

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

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

Use of technology in the classroom

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

- Computers
- Laptops
- Tablets
- Internet

- Online software resources
- Cameras

Prior to using any websites, tools, apps or other online platforms in the classroom, or recommending that pupils use these platforms at home, the class teacher will review and evaluate the resource. Class teachers will ensure that any internet-derived materials are used in line with copyright law.

Pupils will be supervised when using online materials during lesson time – this supervision is suitable to their age and ability. The use of NetSupport by staff during lessons will ensure that pupils online and computer activity can be monitored, and a digital log created, allowing any concerns to be evidenced and easily referred to the DSL.

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 Acceptable Use Agreement for Pupils.

Staff will use all smart technology and personal technology in line with the Acceptable Use Agreement for Staff.

The school recognises that pupils' unlimited and unrestricted access to the internet via mobile phone networks means that some pupils may use the internet in a way which breaches the school's acceptable use of ICT agreement for pupils.

Inappropriate use of smart technology may include:

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

Pupils will not be permitted to use smart devices or any other personal technology whilst in the school and where it is deemed necessary, the school will ban pupil's use of personal technology whilst on school site.

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

Educating parents

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

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

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

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

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

- Parents' evenings
- Parent Workshops
- Newsletters
- Online resources

Internet access

Pupils, staff and other members of the school community will only be granted access to the school's internet network once they have read and signed the Acceptable Use Agreement. A record will be kept of users who have been granted internet access in the school office.

All members of the school community will be encouraged to use the school's internet network, instead of 3G, 4G and 5G networks, as the network has appropriate filtering and monitoring to ensure individuals are using the internet appropriately.

Filtering and monitoring online activity

The Head of IT will ensure the school's ICT network has appropriate filters and monitoring systems in place and that it is meeting the DfE's '[Filtering and monitoring standards for schools and colleges](#)'. The

Head Teacher will ensure 'over blocking' does not lead to unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.

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

The filtering and monitoring systems the school implements will be appropriate to pupils' ages, the number of pupils using the network, how often pupils access the network, and the proportionality of costs compared to the risks. IT subject leaders will undertake monthly checks on the filtering and monitoring systems to ensure they are effective and appropriate.

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

With the use of the NetSupport software, staff are able to identify and block any websites they deem inappropriate for their class.

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

Network security

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

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

All members of staff will have their own unique usernames and private passwords to access the school's systems. Pupils in class, year or key stage year 1 and above will be provided with their own unique username and private passwords. Staff members and pupils will be responsible for keeping

their passwords private. Passwords will have a minimum and maximum length and require a mixture of letters, numbers and symbols to ensure they are as secure as possible.

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

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

Full details of the school's network security measures can be found in the Cyber-security Policy.

The SLT digital lead will be responsible for implementing appropriate network security measures in liaison with the DPO and DSL. Full details of the school's network security measures can be found in the Cyber Security Policy.

Emails

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

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

Staff members and pupils will be required to block spam and junk mail, and report the matter to ICT technicians. The school's monitoring system can detect inappropriate links, malware and profanity within emails – staff and pupils will be made aware of this. Chain letters, spam and all other emails from unknown sources will be deleted without being opened. E-safety lessons will explain what phishing emails and other malicious emails might look like, including information on the following:

- How to determine whether an email address is legitimate
- The types of address a phishing email could use
- The importance of asking "does the email urge you to act immediately?"
- The importance of checking the spelling and grammar of an email

Any cyber-attacks initiated through emails will be managed in line with the Cyber Response and Recovery Plan.

Generative artificial intelligence (AI)

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

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

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

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

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

Social networking

The use of social media by staff and pupils will be managed in line with the school's Social Media Policy.

The school website

The headteacher will be responsible for the overall content of the school website – they will ensure the content is appropriate, accurate, up-to-date and meets government requirements.

The website will be managed in line with the School Website Policy.

Use of devices

Staff members and pupils may be issued with school-owned devices to assist with their work, where necessary. Requirements around the use of school-owned devices can be found in the school's Device User Agreement (appendix 3).

The use of personal devices on the school premises and for the purposes of school work will be managed in line with the Cyber Security Policy.

Remote learning

All remote learning will be delivered in line with the school's Remote Education Policy. This policy specifically sets out how online safety will be considered when delivering remote education.

Monitoring and review

The DPO will review this policy in full every three years, or following any online safety incidents.

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 will include 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 will be 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 will include 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 will be covered in the following curriculum areas: • Relationships education • Computing
Disinformation, misinformation and hoaxes	Some information shared online is accidentally or intentionally wrong, misleading or exaggerated. Teaching will include 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 • Misinformation and understanding that some genuine information can be published with the deliberate intent to harm, e.g. releasing private information or photographs • Online hoaxes, which can be deliberately and inadvertently spread for a variety of reasons	This risk or harm will be covered in the following curriculum areas: • Relationships and health education • Computing

	• 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	
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 will include 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 • The risk of 'too good to be true' online offers, advertising and fake product sales designed to persuade people to part with money for products and services that do not exist	This risk or harm will be covered in the following curriculum areas: • Relationships education • Computing
Online fraud	Fraud can take place online and can have serious consequences for individuals and organisations. Teaching will include the following: • What identity fraud, scams and phishing are • That online fraud can be highly sophisticated and that anyone can be a victim • How to protect yourself and others against different types of online fraud • How to identify 'money mule' schemes and recruiters • The risk of online social engineering to facilitate authorised push payment fraud, where a victim is tricked into sending a payment to the criminal • The risk of sharing personal information that could be used by fraudsters • That children are sometimes targeted to access adults' data • What 'good' companies will and will not do when it comes to personal details • How to report fraud, phishing attempts, suspicious websites and adverts	This risk or harm will be covered in the following curriculum areas: • Relationships education • Computing

Password phishing	Password phishing is the process by which people try to find out individuals' passwords so they can access protected content. Teaching will include the following: • 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	This risk or harm will be covered in the following curriculum areas: • Relationships education • Computing
Personal data	Online platforms and search engines gather personal data – this is often referred to as 'harvesting' or 'farming'. Teaching will include 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 will be covered in the following curriculum areas: • Relationships education • Computing
Persuasive design	Many devices, apps and games are designed to keep users online for longer than they might have planned or desired. Teaching will include 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 to encourage them to spend money or generate advertising revenue • How notifications are used to pull users back online	This risk or harm will be 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 will include the following: • How to find information about privacy settings on various sites, apps, devices and platforms • That privacy settings have limitations	This risk or harm will be covered in the following curriculum areas: • Relationships education • Computing
Targeting of online content	Much of the information seen online is a result of some form of targeting. Teaching will include 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	This risk or harm will be covered in the following curriculum areas: • Relationships education

	• How the targeting is done • The concept of clickbait and how companies can use it to draw people to their sites and services	• 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 will include 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 will be covered in the following curriculum areas: • Relationships education • Computing
Radicalisation	Pupils are at risk of accessing inappropriate and harmful extremist content online, including terrorist material. Extremist and terrorist groups use social media to identify and target vulnerable individuals. Teaching will include the following: • How to recognise extremist behaviour and content online • Which actions could be identified as criminal activity • Techniques used for persuasion • How to access support from trusted individuals and organisations	All areas of the curriculum
Challenges	Online challenges acquire mass followings and encourage others to take part in what they suggest. Teaching will include the following: • What an online challenge is and that, while some will be fun and harmless, others may be dangerous and even illegal • 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	This risk or harm will be covered in the following curriculum areas: • Relationships education

Content which incites violence	Knowing that violence can be incited online and escalate very quickly into offline violence. Teaching will include 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 will be covered in the following curriculum areas: • Relationships education
Fake profiles	Not everyone online is who they say they are. Teaching will include 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 will be covered in the following curriculum areas: • Relationships education • Computing
Grooming	Knowing about the different types of grooming and motivations for it, e.g. radicalisation, child sexual abuse and exploitation, gangs and financial exploitation. Teaching will include the following: • Boundaries in friendships with peers, in families, and with others • Key indicators of grooming behaviour • 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.	This risk or harm will be covered in the following curriculum areas: • Relationships education
Unsafe communication	Knowing different strategies for staying safe when communicating with others, especially people they do not know or have not met. Teaching will include 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	This risk or harm will be covered in the following curriculum areas: • Relationships education • Computing

	What online consent is and how to develop strategies to confidently say no to both friends and strangers online	
Wellbeing		
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 will include 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 - 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 of 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	This risk or harm will be covered in the following curriculum areas: Health education
Online vs. offline behaviours	People can often behave differently online to how they would act face to face. Teaching will include the following: - How and why people can often portray an exaggerated picture of their lives (especially online) and how that can lead to pressure - 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 will be covered in the following curriculum areas: Relationships education
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.	

Appendix B – Progression of Knowledge from PurpleMash Scheme of work.

Year 1

Unit	Aims	Success criteria	Unit End Outcomes
1.1 – Online Safety and Exploring Purple Mash	- To log in safely. - To start to understand the idea of 'ownership' of their creative work.	- Pupils can log in to Purple Mash using their own login. - Pupils have created their own avatar and understand why they are used. - Pupils can add their name to a picture they created on the computer. - Pupils are beginning to develop an understanding of ownership of work online. - Pupils can save work into the My Work folder in Purple Mash and understand that this is a private saving space just for their work.	Emerging: With support, pupils demonstrate an awareness of online safety using their own private usernames and passwords for Purple Mash (Unit 1.1 Lesson 1. Point 6). This can be assisted by using printed login cards. Pupils take ownership of their work and save this in their own private space (Unit 1.1 Lesson 1. Point 16). Expected: Pupils demonstrate an understanding of the importance of online safety, using their own private usernames and passwords for Purple Mash (Unit 1.1 Lesson 1. Point 6). Most pupils will be able to demonstrate an understanding of the reasons for keeping their password private including talking about the meaning of 'private information' (Lesson 1) and actively demonstrate this in lessons (Throughout all lessons in Unit 1.1). Pupils take ownership of their work and will be able to save their work, using a memorable file name, to their own personal space on Purple Mash and understand that this can be retrieved later Unit 1.1 Lesson 1 Point 18.

Unit	Aims	Success criteria	Unit End Outcomes
	- To learn how to find saved work in the Online Work area and find teacher comments. - To learn how to search Purple Mash to find resources.	- Pupils can find their saved work in the Online Work area of Purple Mash. - Pupils can find messages that their teacher has left for them on Purple Mash. - Pupils can search Purple Mash to find resources.	Most pupils will be able to add their name to their picture in lesson 1. In lesson 2, most pupils will be able to explain that their teacher was able to connect with them online to leave a message in Purple Mash. They could contribute to the class discussion relating this to other forms of digital communication. Most pupils will be able to give a simple explanation of the way to word comments online when given the example of their teacher commenting upon their work.
	- To become familiar with the types of resources available in the Topics section. - To become more familiar with the icons used in the resources in the Topics section. - To start to add pictures and text to work.	- Pupils will be able to use the different types of topic templates in the Topics section confidently. - Pupils will be confident with the functionality of the icons in the topic templates. - Pupils will know how to use the different icons and writing cues to add pictures and text to their work.	Throughout this unit most pupils will be able to contribute their ideas about communicating appropriately and relate online and off-line appropriate behaviour. Most pupils will be able to open Purple Mash and use the search bar within Purple Mash to find resources (lesson 2). They can suggest appropriate words to search with to find the results that they are looking for.
	To explore the Tools section of Purple Mash and to learn about the common icons used in	Pupils have explored the Tools section on Purple Mash and become familiar	Exceeding: Pupils demonstrate an understanding of the importance of online safety using their own private usernames and passwords for Purple Mash. Pupils understand the importance of keeping information, such as their usernames and passwords private and actively demonstrate this in lessons. Pupils take ownership of their work and save this in their own private space. Pupils demonstrating greater depth understand the

Unit	Aims	Success criteria	Unit End Outcomes
	Purple Mash for Save, Print, Open, New. - To explore the Games section on Purple Mash. - To understand the importance of logging out when they have finished.	with some of the key icons: Save, Print, Open and New. - Pupils have explored the Games section and looked at Table Toons (2x tables). - Pupils can log out of Purple Mash when they have finished using it and know why that is important.	principle but not the terminology of 'intellectual property' e.g., pupils might say 'I am saving my work, in my folder because I have created it and it belongs to me'.

Year 2

Unit\Lesson	Aims	Success criteria	Unit End Outcomes
2.2 – Online Safety	- To know how to refine searches using the Search tool. - To know how to share work electronically using the display boards. - To use digital technology to share work on Purple Mash to communicate and connect with others locally. - To have some knowledge and understanding about sharing more globally on the Internet.	- Pupils can use the search facility to refine searches on Purple Mash by year group and subject. - Pupils can share the work they have created to a display board. - Pupils understand that the teacher approves work before it is displayed. - Pupils are beginning to understand how things can be shared electronically for others to see both on Purple Mash and the Internet.	Emerging: With support, pupils are beginning to understand how to use the Purple Mash search bar and know the implications of inappropriate searches (Unit 2.2 Lesson 1. Point 1). With support, they can share their work using the display board (Unit 2.2 Lesson 1. Point 16). Furthermore, using 2Respond activities, the pupils develop an understanding of how to use email safely and responsibly (Unit 2.2 Lesson 2. Point 4). They also know how to report inappropriate content to their teacher. Expected: Pupils understand how to use the Purple Mash search bar and know the implications of inappropriate searches (Unit 2.2 Lesson 1. Point 1). Most pupils will be able to explain what a digital footprint is, that it is permanent and their online behaviour influences what it shows (Lesson 3). Most pupils will be able to give reasons for keeping their password safe that include protecting their personal information.

Unit\Lesson	Aims	Success criteria	Unit End Outcomes
	- To introduce Email as a communication tool using 2Respond simulations. - To understand how we talk to others when they are not there in front of us. - To open and send simple online communications in the form of email. - To understand that information put online leaves a digital footprint or trail. - To begin to think critically about the	- Pupils know that Email is a form of digital communication. - Pupils understand how 2Repond can teach them how to use email. - Pupils can open and send an email to a 2Respond character. - Pupils have discussed their own experiences and understanding of what email is used for. - Pupils have discussed what makes us feel happy and what makes us feel sad. - Pupils can explain what a digital footprint is. - Pupils can give examples of things that they would not want to be in their digital footprint.	Most pupils will be able to express the good and bad sides of digital technology. In lesson 3, they can give examples of positive effects on life as well as negative. Pupils add their name to work but show a differentiation between full name and first name only when information is to be shared online. Most pupils will be able to share their work to a displayboard (Lesson 1). By sharing their work using the display board, pupils begin to understand how things are shared electronically (Unit 2.2 Lesson 1. Point 16). Most pupils will be able to open and respond to simulated emails in 2Email (Lesson 2) Most pupils will be able to open and send email responses to simulated emails in 2Email (Unit 2.2 Lesson 2 Point 4). Furthermore, using 2Respond activities the pupils develop an understanding of how to use email safely and responsibly (Unit 2.2 Lesson 2. Point 4). They also know how to report inappropriate content to their teacher. Exceeding: Pupils understand how to use the Purple Mash search bar (Unit 2.2 Lesson 1. Point 1) and for greater depth can refine searches using Boolean search terms (AND, OR, NOT). They know the implications of inappropriate searches. Pupils can share their work using the display board and begin to understand

Unit\Lesson	Aims	Success criteria	Unit End Outcomes
	information they leave online. To identify the steps that can be taken to keep personal data and hardware secure.		how things are shared electronically (Unit 2.2 Lesson 1. Point 16). Furthermore, using 2Respond activities, the pupils develop an understanding of how to use email safely and responsibly (Unit 2.2 Lesson 2. Point 4). They also know how to report inappropriate content to their teacher.
2.5 – Effective Searching, Lesson 2	To gain a better understanding of searching the Internet.	- I can identify the basic parts of a web search engine search page. - I have learnt to read a web search results page. - I can search for answers to a quiz on the Internet.	Emerging: Pupils have an awareness that their Internet searches form part of a 'digital footprint'. Expected: Pupils can relate the creation of a digital footprint to their search history and make contributions to the class discussion about this in relation to online safety. Pupils know that many search engine companies collect and sell information about users. Exceeding: Pupils apply what they know about search engine algorithms to their own online safety and digital footprint. They can understand the implications of search engines selling information and having paid ads at the top of search results.

Year 3

Unit\Lesson	Aims	Success criteria	Unit End Outcomes
3.2 – Online Safety	- To know what makes a safe password, how to keep passwords safe and the consequences of giving your passwords away. - To understand how the Internet can be used to help us to communicate effectively. - To understand how a blog can be used to help us communicate with a wider audience.	- Pupils understand what makes a good password for use on the Internet. Pupils are beginning to realise the outcomes of not keeping passwords safe. - Pupils can contribute to a concept map of all the different ways they know that the Internet can help us to communicate. - Pupils have contributed to a class blog with clear and appropriate messages. - Extension: Pupils understand that passwords help to limit who can see personal / private / confidential information.	Emerging: With prompting, pupils can understand that it is important to have a secure password that is not shared with anyone else (Unit 3.2 Lesson 1. Point 1). Pupils can give a negative example of failure to keep passwords secure (Unit 3.2 Lesson 1. Point 1). Pupils are beginning to identify some of the main things to look for when deciding whether the information on a website is trustworthy or not (Unit 3.2 Lesson 2. Point 2). Expected: Pupils understand the importance of a secure password and not sharing this with anyone else (Unit 3.2 Lesson 1 Point 1). Furthermore, pupils understand the negative implications of failure to keep passwords safe and secure and can suggest examples of good and poor passwords (Unit 3.2 Lesson 1 Point 1). When using the internet, pupils can appraise the accuracy of the information on a website and make decisions on whether it is a trustworthy source of information (Unit 3.2 Lesson 2 Point 2). In lesson 1, step 16, pupils have a choice of topics about which to blog. Most pupils will have gained an understanding that it is not acceptable to use the work of others or post images of others without consent.

Unit\Lesson	Aims	Success criteria	Unit End Outcomes
	• For pupils to consider if what they read on websites is true? • To look at a 'spoof' website. • To create a 'spoof' webpage. • To think about why these sites might exist and how to check that the information is accurate.	• Pupils understand that some information held on websites may not be accurate or true. • Pupils are beginning to understand how to search the Internet and how to think critically about the results that are returned. • Pupils have accessed and assessed a 'spoof' website. • Pupils have created their own 'spoof' webpage mock-up. • Pupils have shared their 'spoof' web page on a class display board. • Extension: Pupils evaluate facts from a website and explain how they fact checked the information that was presented.	Most pupils recognise the PEGI ratings and can give examples of why content is rated and how this protects them (lesson 3) Most pupils can contribute to a class collaborative file about the effects of inappropriate content with useful suggestions (lesson 3). Most pupils can answer the quiz questions in lesson 3, their answers demonstrating that they are developing their understanding of the features of online communication. In lesson 1, their blog posts and comments are appropriate. Most pupils can express the need to tell a trusted adult if they are upset by anything online, in lesson 3 their responses illustrate that they have taken this message onboard. Most pupils will be able to use Purple Mash as a platform for collaboration. Specifically, they will create a spoof website for other pupils to read and share on a class display board (Unit 3.2 Lesson 2). In lesson 2, most pupils can use suitable keywords when trying to verify sources. Exceeding: Pupils demonstrating greater depth will be able to give a clear explanation and examples of why having a secure, confidential password is essential and give negative examples of it not being secure and confidential (Unit 3.2 Lesson 1 Point 1).

Unit\Lesson	Aims	Success criteria	Unit End Outcomes
	• To learn about the meaning of age restrictions symbols on digital media and devices. • To discuss why PEGI restrictions exist. • To know where to turn for help if they see inappropriate content or have inappropriate contact from others.	• Pupils can identify some physical and emotional effects of playing/watching inappropriate content/games. • Pupils relate cyberbullying to bullying in the real-world and have strategies for dealing with online bullying including screenshot and reporting.	Pupils will be able to appraise the accuracy of information shared on a website and provide suitable evidence to support their decisions on whether it is trustworthy or not (Unit 3.2 Lesson 2. Point 2).
Unit 3.5 – Email Lessons 3 and 4	• To learn how to use email safely.	• Pupils have written rules about how to stay safe using email. • Pupils have contributed to classmates' rules. • Pupils understand the importance of draft. • Pupils have created a quiz about email safety which explores scenarios that	Emerging: Pupils demonstrate a basic understanding of email conventions and safety (Unit 3.5 Lesson 3 & 4). Expected: Pupils understand the importance of staying safe (Unit 3.5 Lesson 3. Point 2) when using email and have demonstrated knowledge of this through the writing of class rules for their conduct when using email systems (Unit 3.5 Lesson 3 Point 5). Pupils apply their knowledge of email safety through the creation of a quiz on staying safe when emailing (Unit 3.5 Lesson 4. Point 3). In lesson 3, pupils can suggest why they need to seek permission before sharing photos.

Unit\Lesson	Aims	Success criteria	Unit End Outcomes
		they could come across in the future.	In lesson 1, pupils can refer to what they learnt in Unit 3.2 regarding Online Safety when suggesting the way to communicate appropriately online. Pupils' email messages illustrate that they have taken on board messages about appropriate communication with a regard for their audience. In lesson 3, this forms part of the slideshow discussion., pupils include this as part of their guidelines for step 5. Exceeding: Pupils are not only able to demonstrate an understanding of email conventions and keeping safe but can explain why conventions and certain recognised positive behaviours are expected and the possible consequences of not abiding by them (Unit 3.5 Lessons 3 & 4). Pupils demonstrating greater depth, understand the importance of staying safe (Unit 3.5 Lesson 3. Point 2) when using email and can apply these principles to the related aspects of messaging. Pupils demonstrate their knowledge through taking an active role in the writing of class rules and quiz creation on appropriate conduct when using email systems and can expand on their points to explain their reasoning (Unit 3.5 Lesson 3. Point 5).

Year 4

Unit\Lesson	Aims	Success criteria	Unit End Outcomes
4.2 – Online Safety	- To understand how pupils can protect themselves from online identity theft. - Understand that information put online leaves a digital footprint or trail and that this can aid identity theft. - To identify the risks and benefits of	- Pupils know that security symbols such as a padlock protect their identity online. - Pupils know the meaning of the term 'phishing' and are aware of the existence of scam websites. - Pupils can explain what a digital footprint is and how it relates to identity theft. - Pupils can give examples of things that they would not want to be in their digital footprint. - Pupils can identify possible risks of installing free and paid for software.	Emerging: Pupils contribute their ideas to discussion of spam email (lesson 1), malware (lesson 2) and plagiarism (lesson 3). They have included appropriate content in their Top Tips for Online Safety publication (lesson 2, point 5 and onwards). They have been able to share their work online. With support throughout, pupils show an understand what online safety is. In a small group, they can use 2Connect (Unit 4.2 Lesson 1. Point 3) to map out the key features of online safety. Pupils produce a simple leaflet, postcard, or slideshow etc about online safety, which can then be used as part of presentation to parents (Unit 4.2 Lesson 1. Point 7). Expected: Pupils have decided upon the most important online safety messages to communicate and have shared these ideas in their Top Tips for Online Safety publication (lesson 2, point 5 and onwards). They put this knowledge into action in their own online activity. Pupils can explore key concepts relating to online safety using 2Connect Unit 4.2 Lesson 1. Point 3). They help others to understand the importance of online safety (Unit 4.2 Lesson 2. Point 3) and apply their knowledge through the creation of online

Unit\Lesson	Aims	Success criteria	Unit End Outcomes
	installing software including apps.	- Pupils know that malware is software that is specifically designed to disrupt, damage, or gain access to a computer. - Pupils know what a computer virus is.	safety resources which are then used as part of presentation to parents (Unit 4.2 Lesson 1. Point 7). Using the example from lesson 1, pupils can give some examples of things to look out for in an email to ensure that it from a valid source and is not a phishing scam email. They can explain what can be learnt by looking at the padlock details for a website (lesson 1)
	- To understand that copying the work of others and presenting it as their own is called 'plagiarism' and to consider the consequences of plagiarism. - To identify appropriate behaviour when participating or contributing to collaborative online projects for learning.	- Pupils can determine whether activities that they undertake online, infringe another's' copyright. They know the difference between researching and using information and copying it - Pupils know about citing sources that they have used.	Most pupils can reflect upon positive and negative aspects of a digital footprint and can give examples of the care they would take when sharing online in relation to their and others' digital footprint (lesson 1). Most pupils can give reasons for taking care when installing apps or software. They know what Malware is and the possible impact of computer viruses and can give recommendations for how best to ensure that they only install valid software as part of their top tips document in lesson 2.
	To identify the positive and negative influences of	Pupils can take more informed ownership of the way that they choose	Most pupils can give reasons for limiting screen time that include the effect on physical and mental health. In lesson 4, they were able to reflect on their own screen time and collective class screen time and begin to make informed decisions about when to limit their own screen time.

Unit\Lesson	Aims	Success criteria	Unit End Outcomes
	technology on health and the environment. To understand the importance of balancing game and screen time with other parts of their lives.	to use their free time. They recognise a need to find a balance between being active and digital activities. Pupils can give reasons for limiting screen time.	Most pupils can explain how plagiarism is stealing, they are beginning to be able to identify the aspects of sharing that would be classed as plagiarism (lesson 3) In lesson 4, pupils were able to include actions for reporting cyberbullying or inappropriate content in their screen time study document. By completing lesson 4, most pupils would have saved both online and locally to a device and are able to explain the differences between the two storage types. Most pupils will be able to identify key messages that should be shared with other pupils and parents about online safety, including identification of reliable content from websites found via common search engines (Unit 4.2 Lessons 1 & 2). Exceeding: Pupils have decided upon the most important online safety messages to communicate and have shared these ideas in their Top Tips for Online Safety publication (lesson 2, point 5 and onwards). Pupils demonstrate that they are making connections between the positive possibilities that technology provides e.g. collaboration and sharing and the possible downsides of this such as malware and phishing. They actively use this knowledge to support their own online activities safely. Pupils demonstrating greater depth understand the key concepts and implications of the choices they make relating to online safety

Unit\Lesson	Aims	Success criteria	Unit End Outcomes
			(Unit 4.2 Lesson 1. Point 3). They help others to understand the importance of online safety (Unit 4.2 Lesson 2. Point 3) and apply their knowledge and approach to staying safe online in all areas of the curriculum (Unit 4.2 Lesson 1. Point 7).
4.7 – Effective Searching, lesson 3	To assess whether an information source is true and reliable.	Pupils can analyse the contents of a web page for clues about the credibility of the information.	Emerging: Pupils understand that just because something is on the internet it does not mean it is true. They know that they should consider checking and verifying information. Expected: Most pupils will be able to analyse the contents of a web page for obvious clues about the credibility of the information. They will be able to work in small groups to decide collectively if a website has questionable credibility (Unit 4.7, Lesson 3). Exceeding: Pupils understand that a single search provider might present a bias, or present information from a flawed source. They seek to corroborate information from other sources using more than one search engine. Pupils know that the results presented to a person on many search engines reflect their previous searches. They realise that this does not give a balanced way to form an opinion about something and presents dangers of being consumed by inaccurate viewpoints and having a misrepresentative world view reinforced.

Year 5

Unit\Lesson	Aims	Success criteria	Unit End Outcomes
5.2 – Online Safety	- To gain a greater understanding of the impact that sharing digital content can have. - To review sources of support when using technology. - To review pupils' responsibility to one another in their online behaviour. - To know how to maintain secure passwords. - To understand the advantages, disadvantages, permissions, and purposes of altering an	- I think critically about the information that I share online both about myself and others. - I know who to tell if I am upset by something that happens online. - I can use the SMART rules as a source of guidance when online. - Pupils think critically about what they share online, even when asked by a usually reliable person to share something. - Pupils have clear ideas about good passwords.	Emerging: Pupils demonstrate a developing understanding of their responsibility to others as well as to themselves when communicating and sharing content online. They know what to do if they are upset by online content and know that there are rules such as the SMART rules to protect them (lesson 1). With support throughout, pupils demonstrate an understanding of what the SMART rules are but may find it difficult to apply all of these to using technology safely and respectfully (Unit 5.1 Lesson 1). They can create a simple comic strip to teach other pupils about online safety (Unit 5.2 Lesson 2). Expected: Pupils demonstrate an understanding of their responsibility to others as well as to themselves when communicating and sharing content online. Pupils demonstrate a clear understanding of what the SMART rules are and how they should be applied to using technology safely and respectfully (Unit 5.1 Lesson 1). In lesson 1, step 2, pupils demonstrate that they are developing critical thinking skills in their online experience and know what sorts of inappropriate content should be reported.

Unit\Lesson	Aims	Success criteria	Unit End Outcomes
	image digitally and the reasons for this. To be aware of appropriate and inappropriate text, photographs and videos and the impact of sharing these online.	- Pupils can see how they can use images and digital technology to create effects not possible without technology. - Pupils have experienced how image manipulation could be used to upset them or others even using simple, freely available tools and little specialist knowledge.	They can apply their knowledge in the creation of a comic strip to teach other pupils about online safety (Unit 5.2 Lesson 2). When doing image editing in lesson 2, they were able to see both the positive and negative consequences of technological developments including altering images both in terms of impact upon themselves and impact upon others. In lesson 3, pupils can explain why citations must be considered when using the work of others. They know that there is a convention for recording citations and can put this into practice in their work. In lesson 3, step 11 onwards, pupils' contributions demonstrate a growing awareness of the context of communication and an ability to view the communication from the intended audience's point-of-view. Most pupils will be able demonstrate that they understand what is meant by reliable and can build on their ability to identify reliable content. In lesson 3 while completing the citation writing frame, they were able to recognise that it is not a good idea to rely upon only 1 source for information, for example, the Pacific Tree Octopus example. Exceeding: Pupils are developing a deeper understanding of the interaction of the positive benefits and negative risks of innovative technology. They take advantage of these technologies in their
	- To learn about how to reference sources in their work - To search the Internet with a consideration for the reliability of the results of sources to check validity and understand the impact of incorrect information.	- Pupils can cite all sources when researching and explain the importance of this. - Pupils select keywords and search techniques to find relevant information and increase reliability - Pupils show an understanding of the advantages and	

Unit\Lesson	Aims	Success criteria	Unit End Outcomes
	Ensuring reliability through using different methods of communication	disadvantages of different forms of communication and when it is appropriate to use each.	work but are mindful of protecting themselves and others from harm. Pupils demonstrating greater depth have a detailed knowledge of what the SMART rules are and understand how these are applied to using technology safely and respectfully. Furthermore, they understand the implications of improper use of technology and the internet (Unit 5.1 Lesson 1). They can apply their knowledge in the creation of a detailed comic strip to teach other pupils about online safety (Unit 5.2 Lesson 2).

Year 6

Unit\Lesson	Aims	Success criteria	Unit End Outcomes
6.2 – Online Safety	- Identify benefits and risks of mobile devices broadcasting the location of the user/device, e.g. apps accessing location. - Identify secure sites by looking for privacy seals of approval, e.g. https, padlock icon. - Identify the benefits and risks of giving personal information and device access to different software.	- Pupils have used the example game and further research to refresh their memories about risks online including sharing location, secure websites, spoof websites, phishing and other email scams. - Pupils have used the example game and further research to refresh their memories about the steps they can take to protect themselves including protecting their digital footprint, where to go for help, smart rules and security software.	Emerging: Pupils can refer to the SMART rules to guide them online. They can navigate networks within Purple Mash (Work folders, class folders and group folders), the local network (school) and the Internet (using as a source for research or leisure time). They use these networks to collaborate with support using Purple Mash tools such as 2Write and 2Connect. They can use search tools and have an awareness of the need to select sources carefully. They can recognise features online that are risks and those that exist to protect them (lesson 1). Pupils are aware that their actions online have an impact not only on themselves but on others as well. They know to ask for help if they are worried or distressed by something online. Expected: Pupils have a good knowledge of the benefits and risks to working collaboratively. They have no trouble navigating networks within Purple Mash (Work folders, class folders and group folders), the local network (school) and the Internet (using as a source for research or leisure time). They use these networks to collaborate using Purple Mash tools such as 2Write, 2Connect and 2Blog and can use a variety of networked devices such as

Unit\Lesson	Aims	Success criteria	Unit End Outcomes
	- To review the meaning of a digital footprint and understand how and why people use their information and online presence to create a virtual image of themselves as a user. - To have a clear idea of appropriate online behaviour and how this can protect themselves and others from possible online dangers, bullying and inappropriate behaviour. - To begin to understand how information online can persist and give away details of those who share or modify it.	- Pupils understand how what they share impacts upon themselves and upon others in the long-term. - Pupils know about the consequences of promoting inappropriate content online and how to put a stop to such behaviour when they experience it or witness it as a bystander. Extension: Pupils' actions demonstrate that they also feel a responsibility to others when communicating and sharing content online.	webcams, online tools, printers, and tablets in a connected way for their educational benefit. Pupils can use search tools and routinely try to verify the validity and reliability of their sources. They look for corroborating sources for information and enter keywords that help them to choose the best results. Pupils demonstrate an understanding of their responsibility to others as well as to themselves when communicating and sharing content online. They can identify a variety of risks and benefits of technology (lessons 1 and 3). They feel confident in having strategies to help them promote a positive online image of themselves in their digital footprint. Pupils can identify location sharing as a risk to online safety in lesson 1 and could relate this to work done on protecting their identifying private information. Pupils were able to identify the padlock and https as aids to the online safety in lesson 1 and could explain what these means referring to the work that they did on this in previous years' online safety units. Pupils' work in lesson 1, indicates that they have a clear understanding of terms such as Computer virus, Location sharing, phishing scams, spam email, Malware and Identity theft. In lesson 2, they make sensible contributions to the question of what risks

Unit\Lesson	Aims	Success criteria	Unit End Outcomes
	- To understand the importance of balancing game and screen time with other parts of their lives, e.g. explore the reasons why they may be tempted to spend more time playing games or find it difficult to stop playing and the effect this has on their health. - To identify the positive and negative influences of technology on health and the environment.	- Pupils can take more informed ownership of the way that they choose to use their free time. They recognise a need to find a balance between being active and digital activities. - Pupils can give reasons for limiting screen time. - Pupils can talk about the positives and negative aspects of technology and balance these opposing views. Extension: Pupils have an internalised in-depth understanding of the risks and benefits of an online presence.	there are when installing an App and the possible risks hidden in the small print. Pupils' work as digital footprint detectives in lesson 2 demonstrates that they understand the impact of a positive and negative digital footprint and how to take control of their own online virtual image. Most pupils can balance the positive impact of technology with the reasons for limiting screen time that include the effect on physical and mental health. In lesson 3, they were able to reflect on their own screen time and collective class screen time and begin to make informed decisions about when to limit their own screen time Having studied this aspect in depth in year 5 (lesson 3), pupils routinely include citations in their research work across subjects. They also take care to credit the artist when using images from the Internet. In lesson 2, as part of the discussion surrounding digital footprints, pupils explored the existence of metadata to track the source of images. Having studied this aspect in depth in year 5 (lesson 2, step 11+ and lesson 3, step 6+), pupils take care to credit the artist when using images from the Internet and know how to explore the rights and permissions associated with an image online. They can explain the difference between copyright and privacy and are mindful of both aspects when working with images. Most pupils can make informed choices when communicating online for example selecting the appropriate form of

Unit\Lesson	Aims	Success criteria	Unit End Outcomes
			communication for its purpose and audience. They can discuss the use of instant messaging in social contexts, aware of the pros and cons of using such tools. Exceeding: Pupils view their own/school devices as a means to access a wealth and mixture of networked and local resources. They use these in an integrated way; for example, they can take information and images from one source, compare them to others, include them in their written work alongside their own original images and text to enhance their own understanding and produce high quality comprehensive work. They are implicitly aware of the benefits and risks to working collaboratively. They navigate networks within Purple Mash (Work folders, class folders and group folders), the local network (school) and the Internet and use these networks to collaborate using Purple Mash tools such as 2Write, 2Connect and 2Blog. Pupils can use search tools effectively, routinely verifying the validity and reliability of their sources. They look for corroborating sources for information and enter keywords that help them to choose the most suitable results. They are aware that search engines are also often money-making ventures for their providers and that this has personal privacy implications. They know where to look to investigate their privacy settings on search engines. Pupils have an internalised in-depth understanding of the risks and benefits of an online presence (lessons 1 and 3). Their actions demonstrate that they also feel a responsibility to others when

Unit\Lesson	Aims	Success criteria	Unit End Outcomes
			communicating and sharing content online. They feel confident in having strategies to help them promote a positive online image of themselves and deal with issues that might arise in the future.
6.4 – Blogging, Lesson 4 & 5	• To understand how to contribute to an existing blog. • To understand how and why blog posts are approved by the teacher. • To understand the importance of commenting on blogs. • To peer-assess blogs against the agreed success criteria.	• Pupils can post comments and blog posts to an existing class blog. • Pupils understand the approval process that their posts go through and demonstrate an awareness of the issues surrounding inappropriate posts and cyberbullying. • Pupils can comment on and respond to other blogs. • Pupils can assess the effectiveness and impact of a blog. • Pupils understand that content included in their	Emerging: Pupils are aware there is an approval process that their posts go through and demonstrate an awareness of the issues surrounding inappropriate posts and cyberbullying (Unit 6.4 Lesson 4. Point 6). Pupils understand the importance of being respectful on the internet. Expected: Pupils recognise the approval process that their posts go through and demonstrate an awareness of the issues surrounding inappropriate posts and cyberbullying (Unit 6.4 Lesson 4. Point 6). Pupils become active contributors to a blog, carefully considering their responses to blog posts to ensure that they are always respectful (Unit 6.4 Lesson 4. Point 12). Pupils understand the implications of inappropriate use of the blog. Exceeding: Pupils understand why there is an approval process for any posts and understand the issues surrounding inappropriate posts and cyberbullying (Unit 6.4 Lesson 4. Point 6). Pupils demonstrating greater depth, understand that 2Blog is an introduction to the world of blogging and is a way for the user to become a content creator on the internet. As such the content included in their blog carefully considers the end user (Throughout

Unit\Lesson	Aims	Success criteria	Unit End Outcomes
		blog carefully considers the end user.	Unit). They understand the implications of inappropriate use of the blog and how this relates to the real world.

Appendix 3

	Device:	Device ID:
Loaned to:	Date collected:	Date Returned:

Device loan agreement for staff

1. This agreement is between:

- 1) [Insert your school's name and address] ("the school")
- 2) [Insert staff member name and address] ("the employee" and "I")

It governs the use and care of devices assigned to individual staff members. This agreement covers the period from the date the device is issued through to the return date of the device to the school.

All issued equipment shall remain the sole property of the school and is governed by the school's policies.

1. The school is lending the employee [a laptop/tablet] ("the equipment") for the purpose of [working from home/special project, etc]
 2. This agreement sets the conditions for the employee taking the equipment home.
- I confirm that I have read the terms and conditions set out in the agreement and my signature at the end of this agreement confirms that I have read and agree to these terms.

2. Damage/loss

By signing this agreement I agree to take full responsibility for the equipment issued to me and I have read or heard this agreement read aloud and understand the conditions of the agreement.

I understand that I am responsible for the equipment at all times whether on the school's property or not.

If the equipment is [damaged, lost or stolen], I will immediately inform [insert name of staff member who should be contacted], and I acknowledge that I am responsible for full replacement costs. If the equipment is stolen, I will also immediately inform the police.

I agree to keep the equipment in good condition and to return it to the school on demand from the school in the same condition.

I will not leave the equipment unsupervised in unsecured areas.

3. Unacceptable use

I am aware that the school monitors my activity on the equipment.

I will not carry out any activity that constitutes 'unacceptable use'.

This includes, but is not limited to:

- Accessing, creating, storing or linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
- Sharing confidential information about the school, its pupils, or other members of the school community
- Setting up any software, applications or web services on this device without approval by authorised personnel, or creating or using any programme, tool or item of software designed to interfere with the functioning of the ICT facilities, accounts or data
- Carrying out any activity which defames or disparages the school, or risks bringing the school into disrepute
- Using inappropriate or offensive language

I accept that if I engage in any activity that constitutes 'unacceptable use', I may face disciplinary action in line with the school's policies on [staff discipline/staff code of conduct/etc].

4. Personal use

[Set out your school's approach here – use details from your ICT acceptable use policy.]

I will not use this device for any personal use and will not loan the equipment to any other person.

Or,

I will only use this device for personal use and will not loan the equipment to any other person provided that such use:

- Does not take place during [teaching hours/non-break time]
- Does not constitute 'unacceptable use', as defined above

5. Data protection

I agree to take the following measures to keep the data on the device protected.

- Keep the equipment password-protected - strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Make sure the equipment locks if left inactive for a period of time
- Do not share the equipment among family or friends
- Update antivirus and anti-spyware software as required
- Install the latest updates to operating systems, as prompted

If I need help doing any of the above, I will contact [name of relevant IT staff] on the email [email address of relevant IT staff].

6. Return date

I will return the device in its original condition to [location, e.g. office/IT office] within [insert number of days, e.g. 14 days] of being requested to do so.

I will return the equipment to the school upon resignation, dismissal or if I leave the employment of the school for any other reason.

	Device:	Device ID:
Loaned to:	Date collected:	Date Returned:

7. Consent

If staff are collecting the equipment, insert:

By signing this form, I confirm that I have read and agree to the rules and conditions above.

FULL NAME	
SIGNATURE	
DATE	

8. Returned

If staff are returning the equipment, insert:

I have returned the device and no longer require it. I have ensured that it has been returned in the same condition as I received it (note any issues/change in condition below)

By signing this form, I confirm that I have read and agree to the rules and conditions above.

FULL NAME	
SIGNATURE	
DATE	
NOTES	