THE MULBERRY HOUSE SCHOOL

All Mulberry House School Policies are always to be read and considered in conjunction with the Equal Opportunities, UN Convention on the Rights of the Child, Safeguarding Policy, Data Protection Policy, Behaviour Policy, Anti-bullying Policy, Race Equality and Inclusion Policies

ONLINE SAFETY (E-SAFETY) POLICY

This Policy of Mulberry House School applies to all sections of the school including the Early Years Foundation Stage.

The Mulberry House School is a Rights Respecting School and as Duty Bearers, we take our responsibility seriously and respect the following rights in regards to this policy.

- **Article 2:** All children, regardless of their ethnicity, sex, religion, language and abilities or other status, have rights under the UN Rights of the Child.
- **Article 12**: Every child has the right to express their views, feelings and wishes in all matters affecting them, and to have their views considered and taken seriously.
- **Article 13**: All children must be free to express their thoughts and opinions and have access to all kinds of information.
- **Article 15:** Every child has the right to meet with other children and to join groups and organisations, as long as this does not stop other people from enjoying their rights.
- **Article 17:** Every child has the right to reliable information from a variety of sources, and the media should provide information that children can understand. Governments and institutions must help protect children from materials that could harm them.
- **Article 19:** Governments and Institutions must do all they can to ensure that children are protected from all forms of violence, abuse, neglect and bad treatment by their parents or anyone else who looks after them.
- **Article 23:** A child with a disability has the right to live a full and decent life with dignity and, as far as possible, independence and to play an active part in the community.
- **Article 28:** Every child has the right to an education.
- **Article 29:** Education must develop every child's personality, talents and abilities to the full. It must encourage the child's respect for human rights, as well as respect for their parents, their own and other cultures, and the environment.
- **Article 31:** Every child has the right to relax, play and take part in a wide range of cultural and artistic activities.

Contents

E-SAFETY POLICY 1

Reviewed: SEPT-26
Reviewed by: EB
Next Review Due: SEPT-27

THE MULBERRY HOUSE SCHOOL

Contents 1
1 E-SAFETY: THE ISSUES 4
1.1 Introduction 4
1.2 Benefits of ICT 4
1.3 Risks 4
2 MULBERRY HOUSE SCHOOL E-SAFETY STRATEGIES 6
2.1 Definition and purpose of E-Safety 6
2.2 Elements of e-safety 7
2.3 Roles and responsibilities 8
2.4 Pupils with special needs 10
2.5 Working with parents and carers 10
3.1 Accessing and monitoring the system 12
3.2 Acceptable use policies 12
3.3 Teaching E-Safety 12
3.4 ICT and safe teaching practice 14
Appropriate and Responsible Use of Artificial Intelligence (AI) 17
3.5 Safe use of ICT 18
4 RESPONDING TO INCIDENTS 23
4.1 Policy statement 23
4.2 Intentional access of inappropriate websites by a pupil 24
4.3 Inappropriate use of ICT by staff 24
4.4 Cyber bullying 24
4.5 Risk from inappropriate contacts 26
4.6 Risk from contact with violent extremists 27
4.7 Risk from sites advocating suicide, self-harm and anorexia 27
5 SANCTIONS FOR MISUSE OF SCHOOL ICT 28
5.1 Sanctions for pupils 28
5.2 Sanctions for staff 29
Appendix 1: 31
Acceptable Use Policy for Prep Class pupils 31
Appendix 2 33
Acceptable use policy for staff ..... **Error! Bookmark not defined.**
Access and professional use ..... **Error! Bookmark not defined.**

THE MULBERRY HOUSE SCHOOL

Data protection and system security..... **Error! Bookmark not defined.**
Personal use ..... **Error! Bookmark not defined.**
Appendix 3:..... 36
E-safety incident report form..... 36
Appendix 4: Description of ICT applications 40

E-safety policies should be consistent with related school policies such as anti-bullying and behaviour, Child Protection (Safeguarding), acceptable use of ICT policy as well as the Staff Code of Conduct.

1 E-SAFETY: THE ISSUES

1.1 Introduction

It is the school's policy that the educational and social benefits of the internet and digital media platforms should be promoted, but that this should be balanced against the need to safeguard children. To achieve this, the school has developed an e-safety strategy working in partnership with parents.

This policy provides guidance to achieve this by helping to identify the risks and take action to help children use the internet safely and responsibly. **The designated person for E-Safety is Erika Billmore and use is monitored by CST, an external IT support company. The school also uses Smoothwall for its digital filtering and monitoring systems.**

1.2 Benefits of ICT

ICT and digital media is so universal that it is of huge benefit to children to explore and learn the skills involved in its use in order to prepare themselves for the ever-evolving working environment; it is important that the inherent risks must not reduce the children's use of ICT in lessons and activities. The use of the internet and digital media helps us support children's rights under articles 2, 12 13, 15, 17, 23, 28, 29 and 31 from the UN Convention on the Rights of the Child.

ICT and digital media can make a huge contribution to children's education and social development by:

- raising educational attainment, engaging and motivating pupils to learn and improving their confidence
- improving pupil's research and writing skills
- enabling children with disabilities to overcome communications barriers
- enabling children to be taught "remotely", for example children who are unable to attend school in the case of a nationwide "lockdown"
- improving pupil wellbeing through the social and communications opportunities offered
- providing access to a wide range of educational materials and interactive teaching resources.

1.3 Risks

The risk associated with children using ICT, the internet and digital media platforms can be grouped into 4 categories.

1.3.1 Online Content

The internet contains a vast store of information from all over the world which is predominantly aimed at adult audiences. There is a danger that children may be exposed to inappropriate images such as pornography, information advocating violence, extreme religious views, racism or illegal and anti-social behaviour that they are unable to evaluate in a critical manner. There is also a danger that children may be exposed to misinformation, disinformation and conspiracy theories.

1.3.2 Contact

Chat rooms and other social networking sites and apps can pose a real risk to children as users can take on an alias rather than their real names and can hide their true identity. The sites could potentially be used by adults who pose as children in order to befriend and gain children's trust (known as "grooming") with a view to sexually abusing them.

Children may not be aware of the danger of publishing or disclosing personal information about themselves such as contact details that allow them to be identified or located. They may also inadvertently put other children at risk by posting personal information or photographs without consent.

The internet may also be used as a way of bullying a child, known as cyber bullying. More details on this can be found in section 4.5 of this policy.

1.3.3 Culture

Children need to be taught to use ICT, the internet and digital media platforms in a responsible way, as they may put themselves at risk by:

- becoming involved in inappropriate, anti-social or illegal activities as a result of viewing unsuitable materials or contact with inappropriate people
- using information from the internet in a way that breaches copyright laws
- uploading personal information about themselves, including photographs, on social networking sites without realising they are publishing to a potentially global audience
- cyber bullying (see section 4.5 for further details).
- use of mobile devices to take and distribute inappropriate images of themselves onto the internet. The images can be forwarded to a wide audience.
- children may also be adversely affected by obsessive use of the internet that may have a negative impact on their health, social and emotional development and their educational attainment. They may visit sites that advocate extreme and dangerous behaviour such as self-harm or suicide or violent extremism, and more vulnerable children may be at a high degree of risk from such sites. All children may become desensitised to pornography, violence, sex and drug use or self-harm by regularly viewing these online.

1.3.4 Commerce

Children are vulnerable to unregulated commercial activity on the internet that could have serious financial consequences, such as fraud or identity theft, for themselves and their parents. Depending on digital device settings, they could unknowingly make in-app purchases or they could give out financial information, for example, a parent's credit card details, in response to offers for goods or services without seeing the fraudulent intent. Contact via social networking sites can also be used to persuade children to reveal computer passwords or other information about the family for the purposes of fraud.

2 MULBERRY HOUSE SCHOOL E-SAFETY STRATEGIES

2.1 Definition and purpose of E-Safety

Online safety forms part of the School's wider safeguarding arrangements and contributes to protecting children from harm both online and offline. The School recognises its responsibilities under Keeping Children Safe in Education, the Independent School Standards Regulations, the EYFS Statutory Framework and relevant DfE guidance concerning online safety. Government guidance across the UK highlights the importance of safeguarding children and young people from harmful and inappropriate online material (Department for Education, 2021a; Department of Education, 2020; Scottish Government, 2017; Welsh Government, 2021) and all schools have a responsibility under the Children Act 2004 to safeguard and promote the welfare of pupils, as well as owing a duty of care to children and their parents to provide a safe learning environment. E-safety is a framework of policy, practice, education and technological support that ensures a safe e-learning environment in order to maximise the educational benefits of ICT whilst minimising the associated risks.

An online safety strategy enables the school to create a safe e-learning environment that:

- promotes the acquisition of digital skills across the curriculum
- protects children from harm – children are taught to keep themselves and others safe online and use technology responsibly (our RSHE curriculum promotes digital literacy and critical thinking skills, with staff helping pupils to evaluate online content and challenge the content they view)
- supports the children in using digital tools safely, and with integrity
- safeguards staff in their contact with pupils and their own use of the internet
- ensures the school fulfils its duty of care to pupils
- provides clear expectations for staff and pupils on acceptable use of the internet.

2.2 Elements of e-safety

2.2.1 Safe systems

The school uses the Surf Protect system and ensures a safe e-learning environment where unsuitable sites and content is blocked via the use of filtering software, anti-virus software and internet monitoring systems.

Access to the school internet system should be via individual logins and passwords for staff and pupils wherever possible. Visitors should have permission from the headteacher or online safety co-ordinator to access the system and be given a separate visitors login.

2.2.1a Filtering and Monitoring

The School maintains appropriate filtering and monitoring systems in accordance with current Department for Education filtering and monitoring standards.

Filtering and monitoring systems are reviewed at least annually and whenever significant changes are made to the School's technology infrastructure. Reviews involve the Headteacher, Designated Safeguarding Lead, E-Safety Lead and ICT support providers.

The School recognises that filtering and monitoring form part of its safeguarding responsibilities and are designed to help identify and respond to safeguarding concerns, including cyberbullying, inappropriate content, grooming, extremist material and emerging online risks.

A written record of annual filtering and monitoring reviews will be maintained and reported through the School's safeguarding governance arrangements.

2.2.2 Safe practices

This policy is given to all new staff and parents to ensure that everyone is aware of evolving issues in the digital world, and knows what is expected of them in terms of their own acceptable use of the internet, media platforms, digital systems and other technologies.

2.2.3 Safety awareness

It is vital that children are able to keep themselves and others safe and use the internet responsibly. The school, working in partnership with parents and carers, has an important role in raising pupils' awareness of the potential dangers of using the internet and helping them to develop their own strategies to avoid these risks and keep safe online.

Because many children will have access to the internet at home, this policy should be extended and used by parents and carers in the home environment.

2.3 Roles and responsibilities

2.3.0 Online Safety Governance

Online safety forms part of the School's wider safeguarding framework. The Headteacher, Designated Safeguarding Lead, E-Safety Lead, ICT support providers and Directors share responsibility for maintaining a safe online environment, monitoring emerging risks and ensuring that appropriate filtering, monitoring and cyber security measures remain effective.

2.3.1 Headteacher's role

The Head teacher has ultimate responsibility for e-safety issues within the school including:

- the overall development and implementation of the school's e-safety policy
- ensuring that e-safety issues are given a high profile within the school community
- linking with parents and carers to promote e-safety and promote the school's e-safety strategy
- ensuring e-safety is embedded in the curriculum
- deciding on sanctions against staff and pupils who are in breach of acceptable use policies.

The Headteacher retains overall responsibility for online safety and safeguarding oversight. Online safety is reported to the Directors as part of the School's safeguarding governance arrangements.

2.3.2 E-safety officer's role

The school has a designated e-safety officer who is responsible for co-ordinating e-safety policies on behalf of the school. The named e-safety contact is Erika Billmore, the Headteacher.

The e-safety officer is responsible for:

- developing, implementing, monitoring and reviewing the school's e-safety policy
- ensuring that staff and pupils are aware that any e-safety incident should be reported to them
- providing the first point of contact and advice for school staff, pupils and parents
- liaising with the school's ICT post holders and all teaching staff to ensure they are kept up to date with e-safety issues and to advise of any new trends, incidents and arising problems to the Headteacher

- assessing the impact and risk of emerging technology and the school's response to this in association with the ICT post holders and the Headteacher
- raising the profile of e-safety awareness with the school by ensuring access to training and relevant e-safety literature
- ensuring that all staff and parents have read and signed the acceptable use policy (AUP)
- maintaining a log of internet related incidents and co-ordinate any investigation into breaches
- where appropriate, reporting incidents to relevant local authority safeguarding, online safety or law-enforcement contacts.
- deciding whether or not a referral should be made to Children's Social Care or the Police.

2.3.3 Person responsible for ICT

CST are responsible for:

- supporting the maintenance and monitoring of the school's anti-virus and filtering systems
- carrying out monitoring and audits of networks and reporting breaches to the e-safety officer
- supporting any subsequent investigation into breaches and preserving any evidence, in parallel with the E-Safety Officer and Designated Safeguarding Lead as appropriate

2.3.4 Role of school staff

All staff have a dual role concerning their own internet use and providing guidance, support and supervision for pupils. Their role is:

- adhering to the school's e-safety and acceptable use policy and procedures
- communicating the school's e-safety and acceptable use policy to pupils
- keeping pupils safe and ensuring they receive close supervision and support whilst using the internet during lessons and any free-play activities
- planning careful use of the internet for lessons and researching/vetting/checking online materials and resources, e.g. interactive games as some sites can use pop-ups/advertising banners that are not suitable for children to view
- highlighting the use of any digital media, including devices, specific apps and websites being used for any activity within planning
- reporting breaches of internet use to the e-safety officer

- recognising when pupils are at risk from their internet use or have had negative experiences and taking appropriate action, for example referral to the e-safety officer

2.4 Pupils with special needs

Pupils with learning difficulties or disabilities may be more vulnerable to risk from use of ICT, the internet and digital platforms and could require additional guidance on e-safety practice as well as closer supervision. Schools which discourage or ban the use of IT/electronic media, or whose pupils cannot use them due to disability, may legitimately reflect this in their approach to technological education, but should still ensure that pupils have conceptual familiarity with digital skills and technology which will be encountered in everyday life, eg cars, cash machines and mobile phones

The Special Educational Needs and Disabilities co-ordinator is responsible for coordinating extra support for these pupils and should:

- link with the e-safety officer to discuss and agree whether the mainstream safeguarding systems on the system are adequate for pupils with special educational needs and/or disabilities
- where necessary, liaise with the e-safety officer and the school's ICT coordinator to discuss any requirements for further safeguards to tailored resources and materials in order to meet the needs of the pupils, e.g. specialist hardware or software
- ensure that the school's e-safety policy is adapted to suit the needs of the pupils
- liaise with parents, carers and other relevant agencies in developing e-safety practices for the pupils
- keep up to date with any developments regarding emerging technologies and e-safety and how these may impact on the pupils, e.g. through visiting conferences and exhibitions

2.5 Working with parents and carers

The school realises the importance of involving parents and carers in the development and implementation of our e-safety strategies and policy; most children will have internet access at home and might not be as closely supervised in its use as they would be at school.

Parents should be provided with information on ICT learning and the school's e-safety policy when they are asked to sign acceptable use agreements on behalf of their child so that they are fully aware of their child's level of internet use within the school as well as the school's expectations regarding their behaviour.

Termly newsletters highlight the importance of E-safety and parent talks are held to educate the parents on current matters. An E-safety page on the website further communicates tips for parents on how to keep their children safe online.

THE MULBERRY HOUSE SCHOOL

The Camden Safeguarding Children Partnership (CSCP) online safety leaflet for parents is available on the CSCP website:

https://cscp.org.uk/parents-and-carers/online-safety/

Please see safeguarding policy for relevant contact numbers.

Reviewed: SEPT-26
Reviewed by: EB
Next Review Due: SEPT-27

3 E-SAFETY POLICIES

3.1 Accessing and monitoring the system

- The e-safety officer keeps a record of all logins used within the school for the purposes of monitoring and auditing internet activity.
- The Mulberry House School has web filtering in place which is provided by Exa. Exa provides analytical data which logs every site visited or attempted to visit. The Mulberry House School then stores the data logs for one month.
- The Mulberry House School also has a pro-active safeguarding/ monitoring solution by Smoothwall whereby all devices are monitored throughout the school and reports sent weekly to the Headteacher with further actions.
- All desktop and laptop computer screens face the classroom therefore staff are able to monitor computers easily, i.e. staff make sure that when using laptops they are set up around the edge of the room.
- Staff supervise pupil internet use very closely.

Off Site Access

- "The School must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. This is in relation to data belonging to all members of the school community. As such, no member of staff is permitted to remove sensitive personal data from school premises, whether in paper or electronic form and wherever stored, without prior consent of the Headteacher. Where a member of staff is permitted to download data off site it will need to be password protected."

3.2 Acceptable use policies

- An acceptable use agreement is attached to this policy. Parents should sign this on their child's behalf.
- Staff are expected to sign an acceptable use policy upon on their appointment and this is integrated into their general terms of employment.

A copy of all signed acceptable use agreements are kept on file.

3.3 Teaching E-Safety

3.3.2 Content Be Safe Online

Pupils are taught;

- **The NSPCC Guidance: Be Share Aware: talk about what's OK, and not OK, to share online from entry to the second school.**
- Smartie's top tip: 'Before I tap or click, I need to stop and think… I need to tell someone!' This refers to pop ups, notifications and anything that makes them feel uncomfortable or worried.

- The Breck Foundation's 'Stop, get off and tell' tip. This refers to anything that makes them feel uncomfortable or worried in relation to requests/communication from anyone online, e.g. strangers.
- the benefits and risks of using the internet as a learning tool
- how their behaviour can put themselves and others at risk
- what strategies they can use to keep themselves safe, about what 'personal information' is - such as email address, full name, phone number, address and school name - and why it's important
- simple ways to protect their privacy, i.e. not disclosing passwords, their address, birthdays or other personal information, never sharing images and photos, and what might be appropriate or not
- that it isn't easy to identify someone online and people aren't always who they say they are and that if it is someone who genuinely knows them, that they shouldn't need to ask for their personal information online
- that not all information shared online is factually accurate, exploring topics such as fake news as appropriate
- that some online content may be inaccurate, misleading or deliberately false (misinformation and disinformation) and that they should seek support from a trusted adult if they are unsure whether information can be trusted.
- that some pictures, videos and audio recordings can be altered or generated using Artificial Intelligence (AI) and may not show real events or real people.
- that if they're in any doubt about what they have seen online, they should talk to a teacher or parent immediately and that they are not in trouble.
- what to do if they are concerned about something they have seen or received via the internet
- that the school has a "no blame" policy so that pupils are encouraged to report any e-safety incidents
- that the school has a "no tolerance" policy regarding cyber bullying
- the basic principles of "netiquette" and "Class-Zoom" behaviour for any remote learning
- that behaviour that breaches acceptable use policies will be subject to sanctions and disciplinary action
- that the internet is filtered and monitored, and access to some sites will be blocked for safety
- the dangers of cyber-bullying and sharing content in the digital world (e.g. including sexting) – even if pupils in a particular faith community are not meant to use mobile phones or have limited access to the internet.

3.3.3 Delivering e-safety messages

- All teachers are primarily responsible for delivering an ongoing e-safety education in the classroom as part of the curriculum always consistently reminding the children about how to stay safe online as part of any activities involving internet use.
- Rules regarding safe internet use are displayed in all classrooms and teaching areas where computers are used to deliver lessons.
- The start of every lesson where computers are being used should be an opportunity to remind pupils of expectations on internet use and the need to follow basic principles in order to keep safe.
- Our RSHE curriculum covers the promotion of e-safety and digital literacy. Teachers may wish to use PSHEE lessons/Circle Times as a forum for discussion on e-safety issues to ensure that pupils understand the risks and why it is important to regulate their behaviour whilst online.

3.4 ICT and safe teaching practice

School staff members need to be aware of the importance of maintaining professional standards of behaviour with regards to their own internet use, particularly in relation to their communications with pupils. The School's computers and systems, including the e-mail and internet facilities, are a vital part of its organisation and should be used only by those authorised to do so and only for the proper purposes of the School.

In order to protect the system:

- Introduction or download of software or applications to the system without authorisation is prohibited;
- any attempt to gain unauthorised access to, or to tamper with, any part of any computer system or software or installation will be regarded as gross misconduct; and
- All staff must be vigilant and responsible for the protection the systems from viruses e.g. checking attachments before downloading. The school provides guidance on virus protection.

E-mail and internet access are provided to you only for the School's purpose. Limited, occasional or incidental personal use will be allowed where such personal use is conducted with a sense of responsibility, but the privilege must not be abused. It must have no negative impact on the School and may only take place at times permitted by the Headteacher. Accessing or distributing inappropriate or offensive material is strictly prohibited as it may harm the School's reputation both internally and externally, as well as your own reputation.

If, in the School's opinion, electronic media and services are being used improperly and/or in breach of any aspect of this policy, disciplinary action will be taken, which in serious

cases could lead to dismissal. Misuse of the internet or e-mail or breach of this policy could also lead to civil or criminal actions against you or the organisation.

The following points should be followed by staff to ensure that their behaviour is not open to misinterpretation and to safeguard them from misplaced or malicious allegations.

- Photographs and videos of pupils should only be taken by staff in connection with educational purposes, for example school trips and documenting learning in lessons.
- Photographs and videos should be transferred from devices to the Media drive as soon as possible after their creation and deleted from devices in case of theft, as this would be a very serious safeguarding risk and GDPR breach.
- **Staff must only use school equipment and only store images on the school's secure network and computer system.**
- When making contact with parents or pupils by telephone, staff should only use school equipment. Pupil or parent numbers should not be stored on a staff member's personal device under any circumstances.
- Where staff are using mobile equipment such as laptops provided by the school, they should ensure that the equipment is kept safe and secure at all times and that any damage/operational issues are reported to the SLT and Computing Coordinator / CST IT management services so that they may be resolved in good time.

3.4.1 E-Mails (External and Internal)

You must not write anything in an e-mail that could damage the integrity and reputation of the School or which you cannot justify. Therefore, please do not write or send anything which is insulting, defamatory or discriminatory. Claims of defamation, breach of confidentiality or contract could arise from misuse of the system. You should take care, in particular, in relation to confidential messages using the 'Take Fire' approach before sending an email.

You must not forward any material of a dubious nature that you receive, including chain mails. In order to avoid unnecessary delays to the system, you must not send any personal e-mails attaching pictures, video or sound clips and should delete any such e-mails received.

You must not abuse the e-mail system by transmitting any material in any of the following categories. To do so will constitute gross misconduct and render you liable for summary dismissal in accordance with the School's disciplinary procedure. The (non-exhaustive) list of categories is as follows: -

- defamatory material;
- offensive or obscene material (including any type of pornography);
- any material which is untrue or malicious, including material concerning another member of staff, parent or child at the school;
- any racist, religiously extremist, sexist or disability-biased material.

CCing

Employees should exercise care not to copy e-mails automatically to all those copied in to the original message to which they are replying. Doing so may result in disclosure of confidential information to the wrong person and breach of GDPR.

Monitoring of e-mail

The School reserves the right to monitor employees' e-mails, but will endeavour to inform an affected employee when this is to happen and the reasons for it. The School considers the following to be valid reasons for checking an employee's e-mail:

- If the employee is absent for any reason and communications must be checked for the smooth running of the business to continue.
- If the School suspects that the employee has been viewing or sending offensive or illegal material, such as material containing racist terminology or nudity (although the School understands that it is possible for employees inadvertently to receive such material and they will have the opportunity to explain if this is the case).
- If the School suspects that an employee has been using the e-mail system to send and receive an excessive number of personal communications.
- If the School suspects that the employee is sending or receiving e-mails that are detrimental to the School.
- Access to and use of personal email accounts in school is forbidden and may be blocked. This is to protect pupils from receiving unsolicited mail and preserve the safety of the system from hacking and viruses.

When monitoring e-mails, the School will, save in exceptional circumstances, confine itself to looking at the address and heading of the e-mails. Employees should mark any personal e-mails as such and encourage those who send them to do the same. The School will avoid, where possible, opening e-mails clearly marked as private or personal.

The School reserves the right to retain information that it has gathered on employees' use of e-mail for a period of one year.

3.4.2 Internet

You should never download or transmit (whether internally or externally) or display on your screen any offensive material. For the avoidance of doubt, this includes (but is not limited to) pornography, profanities, and any material that can be interpreted as being racist, sexist or disability-biased in nature. If in doubt as to the suitability of any material, disconnect from the site or close down the e-mail and ask your Team Leader's advice before re-accessing the material. If you do access an inappropriate site in error, disconnect immediately and advise your Team Leader / the E-Safety Officer.

You must take care to ensure that you do not infringe copyright or incur expense to the School, without prior authorisation by your Team Leader, when copying, downloading or sending material to third parties which you have received by e-mail or visited on the internet.

Removing internet access

The School reserves the right to deny internet access to any employee at work, although in such a case it will endeavour to give reasons for doing so.

Registering on websites

Many sites that could be useful for the School require registration. Employees wishing to register as a user of a website for work purposes are encouraged to do so. However, they should ask the Headteacher before doing this. Where teachers require access to blocked websites for educational purposes, this should be discussed and agreed with the e-safety officer. Teachers should notify the e-safety officer once access is no longer needed to ensure the site is blocked.

3.4.3

Appropriate and Responsible Use of Artificial Intelligence (AI)

At The Mulberry House School, we recognise the growing presence of Artificial Intelligence (AI) in education and everyday life. As part of our commitment to safeguarding and digital literacy, we aim to ensure that all members of our school community understand how to use AI tools safely, responsibly, and ethically.

For Pupils:

- Pupils will be introduced to age-appropriate discussions about AI, including what it is and how it is used in the world around them.
- Pupils must not use AI platforms, or AI linked tools or features on learning platforms on an independent basis without adult supervision or explicit permission
- Pupils will be taught to:
    - Think critically about information provided by AI.
    - Understand that AI-generated content may not always be accurate or appropriate.
    - Never share personal information with or through AI tools.
    - Report any inappropriate or concerning content generated by AI to a trusted adult.

For Staff:

- Staff should verify AI-generated content before using it for educational or professional purposes.
- Staff will model responsible use of AI and integrate it into teaching and learning only when it enhances educational outcomes and aligns with safeguarding principles.
- Staff must ensure that any AI tools used:
    - Are age-appropriate and comply with data protection regulations.

- Do not replace critical thinking, creativity, or pupil voice.
- Are used transparently, with clear explanations to pupils about how and why they are being used.

- Staff will receive training and guidance on the ethical use of AI in education.

General Principles:

- AI should never be used to monitor, profile, or make decisions about pupils without human oversight.
- The school will regularly review the use of AI technologies to ensure they align with our safeguarding, data protection, and curriculum policies.
- Parents and carers will be informed about how AI is used in school and supported in understanding its benefits and risks.
- Staff must not enter personal, sensitive or confidential pupil information into public AI systems unless specifically authorised and compliant with the School's data protection arrangements.

Safeguarding Risks Associated with AI

The School recognises that AI technologies may present safeguarding risks including misinformation, disinformation, deepfakes, synthetic media, inappropriate content generation, manipulation and privacy risks.

Staff should report any AI-related safeguarding concerns using the School's safeguarding procedures. Filtering and monitoring arrangements will take account of emerging AI technologies where possible.

3.4.3

Cyber Security

The School recognises that cyber security forms an important part of safeguarding. Appropriate technical measures, access controls, filtering and monitoring systems, security updates and staff awareness measures will be maintained to protect pupils, staff and School information.

Any cyber incident or data breach that may affect safeguarding will be managed promptly and escalated in accordance with the School's safeguarding and data protection procedures.

3.5 Safe use of ICT

3.5.1 Internet and search engines

- Children must be supervised at all times when using the internet.
- Despite filtering systems, it is still possible for pupils to inadvertently access unsuitable websites and content; to reduce risk, teachers should carefully plan use of internet resources ahead of lessons by checking sites and storing information off-line where possible.
- When open searching on the internet, i.e. for images/information on Google, the children should be given key search terms, i.e. fun facts about, the nutritional benefits of, characteristics of... etc. etc.

3.5.2 Evaluating and using internet content

Students should:

- questioning the validity of the source of the information; whether the author's view is objective and what authority they carry
- carrying out comparisons with alternative sources of information
- considering whether the information is current and whether the facts stated are correct.

In addition, pupils should be taught the importance of respecting copyright law and correctly quoting sources and told that plagiarism (copying others work without giving due acknowledgement) is against the rules of the school.

3.5.3 Teaching Practice: Emails

- Access to email systems should be via a class email address only.
- Pupils should be taught not to disclose personal contact details for themselves or others such as addresses or telephone numbers via email correspondence.
- Pupils should be warned that any bullying or harassment via email will not be tolerated and will be dealt with in accordance with the school's anti-bullying policy.
- Pupils should be taught to be wary of opening attachments to emails where they are unsure of the content or have no knowledge of the sender.

3.5.4 Social networking sites, newsgroups and forums

These restrictions are intended to ensure compliance with legal and regulatory restrictions and privacy and confidentiality agreements. Social media includes items such as blogs, podcasts, discussion forums, and social networks. All stakeholders (Staff, Parents and Children) of the School must adhere to the following:

THE MULBERRY HOUSE SCHOOL

State of Social Media

Every Stakeholder can express and communicate an online presence. The Mulberry House School advises its Stakeholders to use the privacy settings when putting it online.

No confidential information relating to the School, staff, pupils or families may be published on social networking sites. Any reference to the School should be professional, respectful and consistent with the Staff Code of Conduct and Social Media expectations.

Responsibility

Material presented online in reference to the Mulberry House School by any Stakeholder must not be made without the written consent of the Headteacher. Posts made in reference to Children, Staff, Parents or other Professionals that a Stakeholder may come in to contact with through the school are strictly prohibited and could result in disciplinary action. At no time must any photographs or materials be published that identify the school or Children and pictures of staff may not be used unless written consent is given by the Headteacher. Any Stakeholder found to be:

1. posting remarks or comments that breach confidentiality and show the school in a negative light
2. deemed to be of a detrimental nature to the company or other Stakeholders
3. posting/publishing photographs of the school, children or staff
4. posting any material that is obscene, defamatory, profane, libellous, threatening, harassing, abusive, hateful, or embarrassing to another person.

All other rules and policies apply here, specifically: respecting colleagues, children, parents, protecting confidentiality, privacy and security, safeguarding and proper use of The Mulberry House School assets.

Employees **must not** under any circumstances engage in social networking with parents and children e.g. do not include parents and children on a social media profile, do not chat online or in private direct communication with parents and children. Staff of Mulberry House School must maintain a professional relationship at all times. Staff should not engage in any conversation with pupils or parents via instant messaging apps.

Stakeholders must not share any of the school's information, disclose any confidential or proprietary information of or about The Mulberry House School, or do anything that might reasonably create the impression that they are communicating on behalf of or as a representative of The Mulberry House School.

For Mulberry House School's and our employees' protection, it is critical that everyone abide by the copyright laws by ensuring that they have permission to use or reproduce any copyrighted text, photos, graphics, video or other material owned by others.

Stakeholders must seek approval from the Headteacher before setting up a Mulberry House School blog or other related social media site.

Company sensitive matters

Any online communication regarding information such as salary, strategic decisions, confidential information deemed inappropriate for uncoordinated public exchange is forbidden.

Topic matter guidelines

The Mulberry House School Stakeholders are encouraged to use the following guidelines in social networking practices. Remember that no information sent over the web is totally secure and as such if you do not wish the information to be made public, refrain from sending it over a social network site.

Even though you may think you are anonymous or use an alias you may be recognised. Maintain professionalism, honesty and respect. Any Stakeholder becomes aware of social networking activity that would be deemed distasteful or fail the good judgment test, please contact the Headteacher.

Company Assets

The use of company assets (computer, internet, email etc.) is intended for purposes relevant to the responsibilities assigned to each employee. Social networking sites are not to be used at any time on the school premises.

Newsgroups and forums are sites that enable users to discuss issues and share ideas online and these may be joined with permission in writing from the Headteacher, with any posts being carefully checked.

- Access to unregulated public social networking sites, newsgroups or forums should be blocked.
- Where schools identify a clear educational use for these sites for online publishing, they should only use approved sites such as those provided by the London Grid for Learning via approved educational platforms.
- Any use of these sites should be strictly supervised by the responsible teacher.
- Pupils should be warned that any bullying or harassment via social networking sites will not be tolerated and will be dealt with in accordance with the school's anti-bullying policy.

3.5.6 Video conferencing

Video conferencing enables users to communicate face-to-face via the internet using web cameras.

- Video conferencing should only take place using School-approved platforms which meet safeguarding, security and data protection requirements.
- Teachers should avoid using other webcam sites on the internet due to the risk of them containing links to adult material. In the event that teachers do use other

webcam sites, this should be discussed and agreed in advance with the Schools IT team.

- Pupil use of video conferencing should be for educational purposes and should be supervised as appropriate to their age. Pupils must ask permission from the responsible teacher before making or receiving a video conference call.
- Video conferencing on platforms such as Zoom may be recorded for Child Protection purposes and in case of any investigations that may arise from this. This will be stored for 6 months to 1 year.
- Teachers should ensure that pupils are appropriately dressed during any photography or filming and equipment must not be used in changing rooms or toilets.
- Photographs and videos may only be downloaded onto the school's computer system with the permission of the network manager and should never enable individual pupils' names or other identifying information to be disclosed.

3.5.7 School website

- Content should not be uploaded onto the school website unless it has been authorised by the e-safety officer and the Headteacher, who are responsible for ensuring that content is accurate, suitable for the purpose and audience, and does not breach copyright or intellectual property law.
- To ensure the privacy and security of staff and pupils, the contact details on the website are the school address, email and telephone number. No contact details for staff or pupils are contained on the website.
- Children's full names should never be published on the website.
- Links to any external websites should be regularly reviewed to ensure that their content is appropriate for the school and the intended audience.

3.5.8 Photographic and video images

- Where the school uses photographs and videos of pupils for publicity purposes, for example on the school website, images should be carefully selected so that individual pupils cannot be easily identified. It is recommended that group photographs are used.
- Written permission is obtained from parents or carers when children first join the school requesting whether the school is able to use photographs, audio recordings or videos of children for website, newsletter and publicity purposes.
- Children's names should never be published where their photograph or video is being used.
- Staff should ensure that children and facial expressions considered are suitably dressed to reduce the risk of inappropriate use of images.
- Images should be securely stored only on the school's computer system and all other copies deleted.

- Stored images should not be labelled with a child's full name.
- Images of children should not leave the premises without the Headteacher's permission.
- When entering the site, children will be recorded on to our CCTV cameras. These images are stored for a period of two weeks and then deleted from the school's system. This footage will only ever be shared under these circumstances;
- Police and other law enforcement agencies where the images recorded could assist in a specific criminal enquiry and / or the prevention of terrorism and disorder.
- Prosecution agencies.
- Appropriate members of School staff (such as Human Resources) in the course of staff or student disciplinary proceedings (including prospective proceedings) to ensure compliance with the School's regulations and policies.
- People whose images have been recorded and retained (unless disclosure to the individual would prejudice criminal enquiries). Images that have been recorded may be viewed on site by the individual whose image has been captured and/or a uniformed police officer when responding to routine incidents which occurred on the same day. No copies may be taken off site.

3.5.9. Mobile Phones

- Parents and Guardians are not permitted to use mobile phones on the school premises
- Staff may only use their mobile phones in the staff rooms of both buildings.

4 RESPONDING TO INCIDENTS

4.1 Policy statement

- All incidents and complaints relating to e-safety and unacceptable internet use will be reported to the e-safety officer in the first instance. All incidents, whether involving pupils or staff, must be recorded by the e-safety officer on the e-safety incident report form (appendix 3).
- Where appropriate, incidents may be reported to relevant safeguarding, online safety, local authority or law-enforcement agencies.
- Where the incident or complaint relates to a member of staff, the matter must always be referred to the Headteacher for action. Incidents involving the Headteacher should be reported to the Founder, Directors, Bethan Lewis Powell and ISI.
- The school's e-safety officer should keep a log of all e-safety incidents and complaints and regularly review the information for evidence of emerging patterns of individual behaviour or weaknesses in the school's e-safety system, and use these to update the e-safety policy.

- E-safety incidents involving safeguarding issues, for example contact with inappropriate adults, should be reported to the designated child protection teacher (where the e-safety officer is not the child protection officer), who will make a decision as to whether or not to refer the matter to the police and/or Safeguarding and Social Care in conjunction with the Headteacher.

Although it is intended that e-safety strategies and polices should reduce the risk to pupils whilst online, this cannot completely rule out the possibility that pupils may access unsuitable material on the internet. Neither the school nor the London Borough of Camden can accept liability for material accessed or any consequences of internet access, but all reasonable precautions will be taken to ensure a safe e-learning environment.

4.2 Intentional access of inappropriate websites by a pupil

- If a pupil deliberately accesses inappropriate or banned websites, they will be in breach of the acceptable use policy and subject to appropriate sanctions (see section 5).
- The incident should be reported to the e-safety officer and details of the website address and URL recorded.
- The e-safety officer should liaise with the ICT co-ordinator to ensure that access to the site is blocked.
- The pupil's parents should be notified of the incident and what action will be taken.

4.3 Inappropriate use of ICT by staff

- If a member of staff witnesses misuse of ICT by a colleague, they should report this to the Headteacher and the e-safety officer immediately.
- The Headteacher should take the computer or laptop out of use and securely store it on order to preserve any evidence. A note of any action taken should be recorded on the e-safety incident report form.
- The e-safety officer should arrange with the IT company to carry out an audit of use to establish which user is responsible and the details of materials accessed.
- Once the facts are established, the Headteacher should take any necessary disciplinary action against the staff member and report the matter to the police where appropriate.
- If the materials viewed are illegal in nature the Headteacher should report the incident to the police and follow their advice, which should also be recorded on the e-safety incident report form.

4.4 Cyber bullying

4.4.1 Definition and description

Cyber bullying is defined as the use of ICT to deliberately hurt or upset someone. Unlike physical forms of bullying, the internet allows bullying to continue past school hours and

invades the victim's home life and personal space. It also allows distribution of hurtful comments and material to a wide audience.

Bullying may take the form of:

- rude, abusive or threatening messages via email or text
- posting insulting, derogatory or defamatory statements on blogs or social networking sites
- setting up websites that specifically target the victim
- making or sharing derogatory or embarrassing videos of someone via mobile phone or email (for example, "happy slapping")
- Creating / sharing inappropriate content, e.g. from generative AI platforms

Cyber bullying can affect pupils and staff members. Often, the internet medium used to perpetrate the bullying allows the bully to remain anonymous. In extreme cases, cyber bullying could be a criminal offence under the Harassment Act 1997 or the Telecommunications Act 1984.

4.4.2 Dealing with incidents

The following covers all incidents of bullying that involve pupils at the school, whether or not they take place on school premises or outside school.

- School anti-bullying and behaviour policies and acceptable use policies should cover the issue of cyber bullying and set out clear expectations of behaviour and sanctions for any breach.
- Any incidents of cyber bullying should be reported to the e-safety officer who will record the incident on the incident report form and ensure that the incident is dealt with in line with the school's anti-bullying policy. Incidents should be monitored and the information used to inform the development of anti-bullying policies.
- Where incidents are extreme, for example threats against someone's life, or continue over a period of time, consideration should be given to reporting the matter to the police as in these cases, the bullying may be a criminal offence.
- As part of e-safety awareness and education, pupils should be told of the "no tolerance" policy for cyber bullying and encouraged to report any incidents to their teacher.
- Evidence of bullying, for example texts, emails or comments on websites should be preserved by the young person as evidence.

4.4.3 Action by service providers

All website providers and mobile phone companies are aware of the issue of cyber bullying and have their own systems in place to deal with problems, such as tracing and blocking communications. Teachers or parents can contact providers at any time for advice on what action can be taken.

- Where the bullying takes place by mobile phone texts, the mobile phone company can be contacted to ask them to trace the calls and ensure that any further calls and texts from that number are blocked. The pupil should also consider changing their phone number.
- Where the bullying takes place by email, and the messages are being sent from a personal email account, contact the service provider so that the sender can be traced and further emails from the sender blocked. The pupil should also consider changing email address.
- Children should be taught to use a 'report' button to report cyberbullying or inappropriate content on a digital platform, where available.
- Where bullying takes place in chat rooms, the pupil should leave the chat room immediately and seek advice from parents or teachers. Bullying should be reported to any chat room moderator to take action.
- Where bullying involves messages on social networking sites or blogs, contact the website provider to request that the comments are removed. In extreme cases, the bully's access to the site can be blocked.
- Parents should be notified of any incidents and advised on what measures they can take to block any offensive messages on computers at home.

4.5 Risk from inappropriate contacts

Teachers may be concerned about a pupil being at risk as a consequence of their contact with an adult they have met over the internet. The pupil may report inappropriate contacts or teachers may suspect that the pupil is being groomed or has arranged to meet with someone they have met online.

- All concerns around inappropriate contacts should be reported to the e-safety officer and the designated child protection teacher.
- The designated child protection teacher should discuss the matter with the referring teacher and where appropriate, speak to the pupil involved, before deciding whether or not to make a referral to Safeguarding and Social Care and/or the police.
- The police should always be contacted if there is a concern that the child is at immediate risk, for example, if they are arranging to meet the adult after school.
- The designated child protection teacher can seek advice on possible courses of action from Camden's e-safety officer in Safeguarding and Social Care.
- Teachers should advise the pupil how to terminate the contact and change contact details where necessary to ensure no further contact.
- The designated child protection teacher and the e-safety officer should always notify the pupil's parents of any concerns or incidents and where appropriate, arrange to meet with them discuss what action they can take to ensure their child's safety.
- Where inappropriate contacts have taken place using school ICT equipment or networks, the e-safety officer should make a note of all actions taken and contact the

IT company to ensure that all evidence is preserved and that an audit of systems is carried out to ensure that the risk to other pupils is minimised.

4.6 Risk from contact with violent extremists

Many extremist groups who advocate violence use the internet as a means of either inciting violence against specific groups or providing information on preparing explosives or carrying out terrorist acts. Because of their personal circumstances, some young people may be susceptible to these influences.

- Staff need to be aware of those pupils who are being targeted by or exposed to harmful influences from violent extremists via the internet. Pupils and staff should be warned of the risks of becoming involved in such groups and informed that accessing such websites is against school policies.
- The school should ensure that adequate filtering is in place and review filtering in response to any incident where a pupil or staff member accesses websites advocating violent extremism.
- All incidents should be dealt with as a breach of the acceptable use policies and the school's behaviour and staff disciplinary procedures should be used as appropriate.
- The e-safety officer and the designated child protection teacher should record and review all incidents in order to establish whether there are any patterns of extremist groups targeting the school and whether current school procedures are robust enough to deal with the issue.
- Pupils and staff know of the risks of becoming involved in groups with extremist ideologies and the tactics they may to groom and exploit. Staff and young people should also be made aware that accessing and sharing certain content is against school policies and certain contact with certain groups is illegal.

Where there are concerns that a young person is being radicalised or is in contact with violent extremists, or that their parents are and this is placing the child or young person at risk, refer to MASH. If there is imminent danger dial 999. In all other circumstances follow the schools safeguarding procedures by speaking to the DSL. If next steps are not clear speak to the Prevent Education Manager or refer directly to MASHadmin@camden.gov.uk.

4.7 Risk from sites advocating suicide, self-harm and anorexia

Some internet sites advocate dangerous activities such as self-harming, suicide or anorexia. Other sites contain sexually explicit material or glorify risky and illegal behaviours like substance misuse. Most young people who visit these sites will not be adversely affected, but some vulnerable, less resilient young people may feel drawn to the sites which may trigger harmful or even fatal behaviours.

- *The school ensures that young people have an opportunity to openly discuss issues such as self-harming, suicide, substance misuse and anorexia as part of the PHSE curriculum.*

- *Pastoral support should be made available to all young people to discuss issues affecting them and to establish whether their online activities are an added risk factor*
- *Staff should receive the training needed to raise awareness of these issues so that they are able to identify those young people who are at risk, offer appropriate support and make appropriate referrals for help.*

5 SANCTIONS FOR MISUSE OF SCHOOL ICT

Sanctions applied should reflect the seriousness of the breach and should take into account all other relevant factors.

5.1 Sanctions for pupils

5.1.1

- use of non-educational sites during lessons
- unauthorised use of email or mobile phones
- unauthorised use of prohibited sites for instant messaging or social networking.

Sanctions will include referral to the class teacher as well as a referral to the e-safety officer.

5.1.2

- continued use of non-educational sites during lessons
- continued unauthorised use of email or mobile phones
- continued use of prohibited sites for instant messaging or social networking
- use of file sharing software
- accidentally corrupting or destroying other people's data without notifying a teacher
- accidentally accessing offensive material without notifying a teacher.

Sanctions include:

- referral to class teacher
- referral to e-safety officer
- loss of internet access for a period of time
- contacting parents.

5.1.3

- deliberately bypassing security or access
- deliberate misuse of generative AI platforms
- deliberately corrupting or destroying other people's data or violating other's privacy

- cyber bullying
- deliberately accessing, sending or distributing offensive or pornographic material
- transmission of commercial or advertising material.

Sanctions include:

- referral to class teacher
- referral to e-safety officer
- referral to Headteacher
- loss of access to the internet for a period of time
- contact with parents
- any sanctions agreed under other school policies

5.1.4

- persistent and/or extreme cyber bullying
- deliberately accessing, downloading or disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- receipt or transmission of material that infringes the copyright of other people or is in breach of the Data Protection Act
- bringing the school name into disrepute.

Sanctions include:

- referral to Headteacher
- contact with parents
- possible exclusion
- removal of equipment
- referral to community police officer
- referral to Camden's e-safety officer.

5.2 Sanctions for staff

These should reflect the seriousness with which any breach of acceptable use policies by staff members will be viewed given their position of trust and the need to ensure acceptable standards of behaviour by adults who work with children.

5.2.1

These are minor breaches of the school's acceptable use policy which amount to misconduct and will be dealt with internally by the Headteacher.

- use of internet for personal activities not connected to professional development
- use of personal data storage media (e.g. removable memory sticks) without carrying out virus checks
- any behaviour on the world wide web that compromises the staff member's professional standing in the school and community, for example inappropriate comments about the school, staff or pupils or inappropriate material published on social networking sites
- sharing or disclosing passwords to others or using other users' passwords
- breaching copyright or licence by installing unlicensed software.

Possible sanctions include referral to the Headteacher who will issue a warning.

5.2.2

These infringements involve deliberate actions that undermine safety and activities that call into question the person's suitability to work with children. They represent gross misconduct that would require a strong response and possible referral to other agencies such as the LADO, police or Safeguarding and Social Care.

- serious misuse of or deliberate damage to any school computer hardware or software, for example deleting files, downloading unsuitable applications
- any deliberate attempt to breach data protection or computer security rules, for example hacking
- deliberately accessing, downloading or disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- receipt or transmission of material that infringes the copyright of other people or is in breach of the Data Protection Act
- bringing the school name into disrepute.

Possible sanctions include:

- referral to the Headteacher
- removal of equipment
- referral to Camden's e-safety officer
- referral to SSC or police
- suspension pending investigation
- disciplinary action in line with school policies

THE MULBERRY HOUSE SCHOOL

Appendix 1:

Acceptable Use Policy for Prep Class pupils

Name:

Class:

I want to stay safe while I am using a computer and I know that anything I do on the computer may be seen by someone else.

I will:

- keep my password a secret
- only open web pages and programs/applications which my teachers have said are okay
- tell my teacher if anything makes me feel scared or uncomfortable
- make sure that any messages I send are polite
- tell my teacher if I get a nasty message
- not reply to any nasty message which makes me feel upset or uncomfortable
- understand that not everything online is true and that I should check with a trusted adult if I am unsure.
- will tell a trusted adult if I see anything online that worries or upsets me.
- understand that some pictures, videos and information online may be created using Artificial Intelligence (AI).
- not give my mobile number, home number or address to anyone
- ask permission before using the internet
- understand that I must not bring software or disks into school without permission
- not use school computers for email
- not use internet chat sites
- understand that the school may check my computer files and the internet sites I visit
- understand that if I deliberately break these rules, I may not be allowed to use the internet or computers.

THE MULBERRY HOUSE SCHOOL

Parents

- □ I have read the above school rules for responsible internet use with my child and agree that my child may have access to the internet. I understand that the school will take all reasonable precautions to ensure pupils do not have access to inappropriate websites, and that the school cannot be held responsible if pupils do access inappropriate websites.
- □ I agree that my child's work can be published on the school website.

Name of child: .....

Parent's name: .....

Signed: .....

Date: .....

THE MULBERRY HOUSE SCHOOL

Appendix 2

E-Safety - Acceptable Use Policy for Staff

Access and Professional Use

- All computer networks and systems belong to the school and are made available to staff for educational, professional and administrative purposes only.
- Staff are expected to abide by all school e-safety rules and the terms of this acceptable use policy. Failure to do so may result in disciplinary action being taken.
- The School uses filtering and monitoring systems. The school reserves the right to monitor all network and internet activity, and to examine and delete files from the school's system.
- Staff have a responsibility to safeguard pupils in their use of the internet, reporting all e-safety concerns to the e-Safety Officer.
- Copyright and intellectual property rights in relation to materials used from the internet must be respected.
- E-mails and other written communications must be professional and appropriate. Staff must not engage in over-familiar or informal messaging within their written communications. All communications should be checked for spelling and grammar errors.
- Staff are not permitted to engage in personal written communications with parents or pupils, including via personal devices or social media. All communications should go through the school office.
- Anonymous messages and the forwarding of chain letters are not permitted.
- The use of chat rooms and access to personal email accounts or social networking sites and blogs is not allowed.
- Staff must be vigilant to emerging online risks including misinformation, disinformation, and conspiracy content. Any concerns should be reported to the e-Safety Officer or Designated Safeguarding Lead.
- Staff must not use generative AI tools (e.g., ChatGPT or image and video generators) with pupils unless approved by the Headteacher and in line with the school's AI Usage Policy. All internet use is subject to filtering and monitoring, including AI-related content.
- Staff must complete annual e-safety and data protection training as part of their safeguarding responsibilities.

THE MULBERRY HOUSE SCHOOL

Data Protection and System Security

- Staff must follow cyber security protocols including strong password use, regular password updates, and secure storage of devices. ***Any suspected breach must be reported immediately***.
- Staff must not share any email or other such digital platform details associated with the School, nor any personal system access details (e.g. user name and password), at any time.
- Staff must comply with the school's Data Protection Policy, including lawful data processing, retention schedules, and responding to any Subject Access Requests. Personal data must not be stored on unapproved devices.
- The use of any portable media such as USB sticks is not allowed without written consent from the Headteacher.
- Personal devices must not be used at any time to access or store School data unless explicitly authorised by the Headteacher and secured in line with the School's policies.
- Staff should ensure that any personal data sent over the internet is encrypted or sent via secure systems. Where personal data is taken off the school premises via laptops, devices and other mobile systems, the information must be encrypted beforehand. Staff must not transfer, send, download or access the School's data without written consent from the Headteacher.
- All photographs should be uploaded to the School's media drive and wiped from device memory cards after their use. On iPads, where photographs are linked to e-profiles, these may remain within the device - strict device password and locked storage protocols must be followed.
- Downloading executable files or unapproved system utilities will not be allowed, and files saved on the School's devices and network may be checked.
- Files should be saved, stored and deleted in line with the School's policies.

Personal Use

- Staff should not browse, download or send material that could be considered offensive to colleagues and pupils or is illegal.
- Staff should not allow school equipment or systems to be used or accessed by unauthorised persons and must keep all computers and devices safe. Staff must also ensure that where they have written authorisation from the Headteacher to use a School device at home, that this is kept safely locked away when not in use.
- Staff should ensure that any personal websites or blogs do not contain material that compromises their professional standing or brings the school's name into disrepute.

THE MULBERRY HOUSE SCHOOL

Any reference to the Mulberry House School, e.g. as part of networking events or educational blogs, must be authorised in writing by the Headteacher.

- The School's internet access must not be used for private purposes during working hours.

I have read the above policy and agree to abide by its terms.

Name: .....

Signed: .....

Date: .....

THE MULBERRY HOUSE SCHOOL

Appendix 3:

E-safety incident report form

This form should be kept on file and a copy emailed to the relevant local authority, safeguarding, online safety or law-enforcement contacts.

School/organisation's details:

Name of school/organisation: **Address:** **Name of e-safety officer:** **Contact details:**

Details of incident

Date: **Time:** **Name of person reporting incident:** If not reported, how was the incident identified? **Where did the incident occur?** □ In school/service setting □ Outside school/service setting **Who was involved in the incident?**

THE MULBERRY HOUSE SCHOOL

□ child/young person □ staff member □ other (please specify

Type of incident:

□ bullying or harassment (cyber bullying)

□ AI-generated content concern

□ deep-fake or manipulated image/video

□ misinformation/disinformation

□ cyber security incident

□ deliberately bypassing security or access

□ data breach

□ hacking or virus propagation

□ racist, sexist, homophobic or religious hate material

□ terrorist material

□ drug/bomb making material

□ child abuse images

□ online gambling

□ soft core pornographic material

□ illegal hard core pornographic material

□ other (please specify)

Description of incident

Nature of incident

□ **Deliberate access**

Did the incident involve material being;

□ created □ viewed □ printed □ shown to others

□ transmitted to others □ distributed

Could the incident be considered as;

□ harassment □ grooming □ cyber bullying □ breach of AUP

□ **Accidental access**

Did the incident involve material being;

□ created □ viewed □ printed □ shown to others

□ transmitted to others □ distributed

Action taken

□ **Staff**

□ incident reported to Headteacher/senior manager

□ advice sought from Safeguarding and Social Care

□ referral made to Safeguarding and Social Care

□ incident reported to police

□ incident reported to Internet Watch Foundation

□ incident reported to IT

□ disciplinary action to be taken

□ e-safety policy to be reviewed/amended

Please detail any specific action taken (ie: removal of equipment)

□ **Child/young person**

□ incident reported to Headteacher/senior manager

□ advice sought from Safeguarding and Social Care

□ referral made to Safeguarding and Social Care

□ incident reported to police

THE MULBERRY HOUSE SCHOOL

□ incident reported to social networking site

□ incident reported to IT

□ child's parents informed

□ disciplinary action to be taken

□ child/young person debriefed

□ e-safety policy to be reviewed/amended

Outcome of incident/investigation

THE MULBERRY HOUSE SCHOOL

Appendix 4: Description of ICT applications

Technology/ Application	Description/ Usage	Benefits	Risks
Internet	◆ Enables the storage, publication and retrieval of a vast range of information ◆ Supports communications systems	◆ Provides access to a wide range of educational materials, information and resources to support learning ◆ Enables pupils and staff to communicate widely with others ◆ Enhances schools management information and business administration systems.	◆ Information is predominantly for an adult audience and may be unsuitable for children ◆ The vast array of information makes retrieval difficult without good research skills and ability to critically evaluate information ◆ Access to sites promoting illegal or anti-social activities, extreme views or commercial and gambling sites.
Email	◆ Allows written communications over the network and the ability to attach documents.	◆ Enables exchange of information and ideas and supports collaborative working. ◆ Enhances written communications skills ◆ A good form of communication for children with some disabilities.	◆ Difficulties controlling contacts and content ◆ Use as a platform for bullying and harassment ◆ Risks from unwanted spam mail, particularly for fraudulent purposes or to introduce viruses to systems ◆ Hacking ◆ Unsolicited mail.
Artificial Intelligence (AI)	◆ Generates text, images, audio and other content using machine learning technology.	◆ Supports learning, creativity, research and administrative efficiency when used appropriately.	◆ Misinformation, disinformation, deepfakes, inappropriate content generation, privacy concerns

Reviewed: Oct-24
Reviewed by: EB/VP
Next Review Due: Oct-25

THE MULBERRY HOUSE SCHOOL

			and over-reliance on AI-generated information.
Chat/instant messaging	◆ Chat rooms allow users to chat online in real time in virtual meeting places with a number of people; ◆ Instant messaging allows real-time chat for 2 people privately with no-one else able to join. Users have control over who they contact through "buddy lists".	◆ Enhances social development by allowing children to exchange experiences and ideas and form friendships with peers. ◆ Use of pseudonyms protects the child's identity. ◆ Moderated chat rooms can offer some protection to children.	◆ Anonymity means that children are not aware of who they are really talking to. ◆ Chat rooms may be used by predatory adults to contact, groom and abuse children online. ◆ Risk of children giving away personal information that may identify or locate them. ◆ May be used as a platform to bully or harass.
Social networking sites	◆ Online communities, including blogs and podcasts, where users can share text, photos and music with others by posting items onto the site and through messaging. ◆ It allows creation of individual profiles. ◆ Users can develop friends lists to allow access to individual profiles and invite comment.	◆ Allows children to network with peers and join forums to exchange ideas and resources. ◆ It provides a creative outlet and improves ICT skills.	◆ Open access means children are at risk of unsuitable contact. ◆ Risk of children posting unsuitable material online that may be manipulated to cause them embarrassment or distress. ◆ Children may post personal information that allows them to be contacted or located. ◆ May be used as a platform to bully or harass.
File sharing (peer-to-peer networking)	◆ Allows users to share computer capability, networks and file storage.	◆ Allows children to network within a community of peers with similar interests and	◆ Illegal download and copyright infringement. ◆ Exposure to unsuitable or

THE MULBERRY HOUSE SCHOOL

	◆ Used to share music, video and other materials.	exchange materials.	illegal materials. ◆ Computers are vulnerable to viruses and hacking.
Mobile phones and multi-media equipment	◆ Mobile phones now carry other functions such as cameras, video-messaging and access to internet and email.	◆ Provide children with a good means of communication and entertainment. ◆ They can also keep children safe and allow them to be contacted or stay in contact.	◆ Their mobile nature makes supervision of use difficult leading to risks of unsuitable contacts or exposure to unsuitable material on the internet or through messaging. ◆ Risk from violent crime due to theft. ◆ Risk of cyberbullying via mobile phones. ◆ Control of photographs to ensure use within the school only or where we have specific permission to do so otherwise.
Digital Cameras	◆ Allows user to upload images and share them with others.	◆ Record of children's achievements. ◆ Sharing of achievements with parents. ◆ Recording work and ideas, creating artwork, documenting experiences for review in lessons such as PE, PHSEE and Recount Writing.	◆ Control of photographs to ensure use within the school only or where we have specific permission to do so otherwise.

THE MULBERRY HOUSE SCHOOL

Reviewed: Oct-24
Reviewed by: EB/VP
Next Review Due: Oct-25