Millbrook Junior School
Dream, Believe, Aspire, Achieve

Millbrook Junior School

Online Safety Policy

This policy was approved by the Governors/Trustees on 5th October 2023

Chair of Governors/Trustees

Online Safety (e-safety) Policy

	Details	Date
Policy Approved By		
Online Safety Policy Reviewed	Annually or in the event of serious Online Safety incident, or in light of important changes legislation or government guidance	
Ofsted Inspection Guidance Online Safety Officer Job Description Filtering Guidance Password Guidance Social Media Guidance School's Social Media Concerns Form AUPs Online Safety and the Law Dealing Online Safety Incidents Useful Links Online Safety Coverage Protecting Data Use of Personal Devices Guidance Keeping Children Safe in Education Sept 2023 – Annex C Online Safety Online Safety and GDPR Questions from the Governing board gov.uk publication	Appendix 1 Appendix 3 Appendix 6 Appendix 7 Appendix 8 Appendix 8a Appendix 9 Appendix 10 Appendix 11 Appendix 12 Appendix 13 Appendix 14 Appendix 15 Appendix 16 Appendix 17 Appendix 18 Appendix 19	

The term e-safety has now been replaced with the broader term Online Safety. Online safety is currently covered by the current Ofsted safeguarding guidelines (see Appendix 1).

Online Safety Policy:

- Millbrook Junior School's Online Safety Policy and agreements apply to all pupils, staff, support staff, external contractors and members of the wider school community who use, have access to or maintain school and school related Internet, computer systems and mobile technologies internally and externally.
- Millbrook Junior School will make reasonable use of relevant legislation and guidelines to affect positive behaviour regarding ICT and Internet usage both on and off the school site. This will include imposing sanctions for inappropriate behaviour – as defined as regulation of student behaviour under the Education and Inspections Act 2006. 'In Loco Parentis' provision under the Children Act 1989 (updated 2004) also allows the school to report and act on instances of cyber bullying, abuse, harassment (including sexual harassment), malicious communication and grossly offensive material; including reporting to the police, social media websites, and hosting providers on behalf of pupils.

- Online Safety policy is a result of a continuous cycle of evaluation and review based on new initiatives, and partnership discussion with stakeholders and outside organisations; technological and Internet developments, current government guidance and school related Online Safety incidents. The policy development cycle develops good practice within the teaching curriculum and wider pastoral curriculum. Regular assessment of strengths and weaknesses help determine inset provision for staff and governors and guidance provided to parents, pupils and local partnerships.

The Online Safety policy covers the use of:

- School based ICT systems and equipment
- School based intranet and networking
- School related external Internet, including but not exclusively, extranet, e-learning platforms, blogs, social media websites
- External access to internal school networking, such as webmail, network access, file-serving (document folders) and printing.
- School ICT equipment off-site, for example staff laptops, digital cameras, mobile phones, tablets, etc.
- Pupil and staff personal ICT equipment when used in school and which makes use of school networking, file-serving or Internet facilities.
- Tablets, mobile phones, smart devices and laptops when used on the school site.

Responsibilities

School Management and Online Safety

- Millbrook Junior School senior leadership is responsible for determining, evaluating and reviewing Online Safety policies to encompass teaching and learning, use of school IT equipment and facilities by pupils, staff and visitors, and agreed criteria for acceptable use by pupils, school staff and governors of Internet capable equipment for school related purposes or in situations which will impact on the reputation of the school, and/or on school premises.
- To ensure Online Safety provision is always designed to encourage positive behaviours and practical real-world strategies for all members of the school and wider school community.
- Leadership is encouraged to be aspirational and innovative in developing strategies for Online Safety provision.

The school Online Safety Officer:

- The school has a designated Online Safety officer, (Kelly Pearson), who reports each term to the SLT and Governors and coordinates Online Safety provision across the school and wider school community.
- The Online Safety officer job description is detailed in Appendix 3
- The Online Safety Officer is responsible for Online Safety issues on a day to day basis and also liaises with school ICT support.
- The Online Safety lead will take lead responsibility for understanding the filtering and monitoring systems and processes in place.
- The Online Safety Officer maintains a log of pupil Online Safety reports and incidents and cross-references these with Safeguarding records. From 10th July 2020, the Deputy Head (Karen Harrison) will maintain a log of staff Online Safety reports and incidents.
- The Online Safety Officer audits and assesses inset requirements for staff and support

staff and ensures that all staff are aware of their responsibilities and the school's Online Safety procedures. The Officer is also the first port of call for staff requiring advice on Online Safety matters.

- The Online Safety Officer is responsible for promoting best practice in Online Safety within the wider school community, including providing and being a source of information for parents and partner stakeholders.
- The Online Safety Officer (along with IT support and the computing coordinator) should be involved in any risk assessment of new technologies, services or software to analyse any potential risks

The technical staff's responsibility:

- That the school's IT infrastructure is secure and not open to misuse or malicious attack and are not open to abuse or unauthorised external access, with particular regard to external logins and wireless networking.
- That anti-virus software is installed and maintained on all school machines and portable devices
- That the school's filtering guidance (Appendix 6) is applied and updated on a regular basis and that responsibility for its implementation is shared with the Online Safety Lead and Designated Safeguarding Lead (DSL)
- That any problems or faults relating to filtering are reported to DSL and to the broadband/filtering provider immediately and recorded on the Online Safety Log
- When testing filtering, test user accounts must be used (test admin, test teacher, test pupil)
- That users may only access the school's network through a rigorously enforced password protection guidance (Appendix 7)
- That he/she keeps up to date with online safety technical information in order to maintain the security of the school network and safeguard children and young people
- That the use of the school network is regularly monitored in order that any deliberate or accidental misuse can be reported to the Online Safety Lead.
- They need to be aware of current thinking and trends in IT security and ensure that the school system, particularly file-sharing and access to the Internet is secure
- Support staff also need to maintain and enforce the school's password policy and monitor and maintain the Internet filtering.
- External contractors, such as VLE providers, website designers/hosts and maintenance contractors should be made fully aware of and agree to the school's Online Safety Policy. Where contractors have access to sensitive school information and material covered by the Data Protection Act, the school will ensure that the contractual agreement and contractor's staff code of conduct, when taken together, are sufficiently robust to provide the required protection for any personal data processed on behalf of the school. The school will not enter into an arrangement with a contractor that involves the processing of personal data if it cannot satisfy itself that the personal data will be processed securely and in accordance with the appropriate laws.

Teaching and teaching support staff:

- Teaching and teaching support staff need to ensure that they are aware of the current school Online Safety policy, practices and associated procedures for reporting Online Safety incidents.

- Teaching and teaching support staff will be provided with Online Safety induction as part of the overall staff induction procedures.
- All staff need to ensure that they have read, understood and signed (thereby indicating an agreement) the Acceptable Use Policy
- All staff need to follow the school's social media guidance (Appendix 8, in regard to external off-site use, personal use (mindful of not bringing the school into disrepute), possible contractual obligations, and conduct on Internet school messaging or communication platforms, for example email, VLE messages and forums and the school website.
- All teaching staff need to monitor pupil Internet and computer usage during lessons in line with this policy.
- Teaching staff should promote best practice regarding avoiding copyright infringement and plagiarism.
- Be aware of online propaganda and help pupils with critical evaluation of online materials.
- Internet usage and suggested websites should be pre-vetted and documented in lesson planning.
- If using their personal device in school, they comply with the school's Use of Personal Mobile Devices guidance (Appendix 16)
- Follow guidance on dealing with Online Safety Incidents (Appendix 9)

Online Safety Designated Safeguarding Lead (DSL):

- The Online Safety DSL is Safeguarding trained (Kelly Pearson July 2021, refreshed July 2023)
- The Online Safety DSL needs to be able to differentiate which Online Safety incidents are required to be reported to CEOP, local Police, LADO, Local Safeguarding Children's Board, social services and parents/guardians.
- Possible scenarios might include:
    - Computer crime – for example hacking of school systems.
    - Allegations or evidence of 'grooming'.
    - Allegations or evidence of cyber bullying in the form of threats of violence, harassment or a malicious communication.
    - Producing and sharing of Youth Produced Sexual Imagery (YPSI)

Pupils:

- Are required to use school Internet and computer systems in agreement with the terms specified in the school Acceptable Use Policies. Pupils are expected to sign the policy to indicate agreement
- Pupils need to be aware of how to report Online Safety incidents in school, and how to use external reporting facilities, such as the Click CEOP button or Childline number.
- Pupils need to be aware that school Acceptable Use Policies cover all computer, Internet and mobile technology usage in school, including the use of personal items such as phones.

Parents and Guardians:

- Parents and guardians need to support the school's stance on promoting good Internet behaviour and responsible use of IT equipment and mobile technologies both at school and at home.

- Millbrook Junior School will provide opportunities to educate parents with regard to Online Safety.

Online Safety Education
Pupils – curriculum teaching:

- How to deal with cyber bullying, how to report cyber bullying, the social effects of spending too much time online and knowing where to go for help.
- Activities, assemblies, year group presentations
- Safer Internet Day.
- The AUP will be signed by pupils at the start of each academic year

Parents and wider community – information, presentation, collaborative meetings and events may include:

- Online Safety information directly delivered to parents: letters, newsletters, Parentmail, website subscribed news emails, software Apps, website.
- Parents Evenings, open days, transition evenings and other events
- Twilight sessions, and/or presentations run by the school for parents and wider school community stakeholders.

Staff – inset and training may include:

- Letters, newsletters, website subscribed news emails, the school extranet and website.
- The Online Safety policy will be updated at the beginning of each academic year
- The Online Safety Officer should be the first port of call for staff requiring Online Safety advice.
- The AUP will be signed by staff at the start of each academic year
- All staff will receive training on the expectations, applicable roles and responsibilities in relation to filtering and monitoring, this will be reviewed with all staff yearly.

Filtering and Security:

- The Filtering provider is the first port of call for advice regarding filtering.
- The school's Internet service is provided by a fully accredited ISP (Schools Broadband). Accredited filtering (Netsweeper by SBB) is used. The school is able to differentiate the levels of filtering based on pupil age, maturity, responsibility; and staff use. The filtering reports and logs should be examined daily, and if possible there should be a facility to monitor 'on the fly'. Classroom management systems should be utilised by teaching staff to monitor all pupil's screens on one staff screen or IWB. Any filtering 'incidents' are examined and action is taken and recorded to prevent a reoccurrence.
- Filtering and monitoring needs to reflect real life rather than being a 'lock down' system. If locked down, or white-list only, the school risks simply transferring Online Safety problems incidents elsewhere – for example to mobile phones, or home usage. The problem is not being dealt with and good behaviours are not being taught. Pupils need to be taught positive responsible behaviour to carry forward into the workplace.
- Password guidance given in Appendix 7

Use of IT facilities for curriculum teaching and learning:

Use of the Internet and IT facilities should be clearly planned prior to the activity. Websites and software Apps should be suggested and provided. Students should be trusted to be responsible when researching the Internet, but the filtering software needs to be flexible enough to allow teaching staff to request manual changes to filter by category as well as specific site depending on the age and maturity of the students.

Use of images and videos and advice on creating a photo permissions agreement:

- In terms of Online Safety, schools must ensure images and videos of pupils, staff, pupil's work and any other personally identifying material must be used, stored, archived, and published in line with GDPR and the Data Protection Act (See Appendix 11), ICO guidance for schools, gov.uk guidance for schools for teacher and the schools AUP.
- There are no laws preventing the taking of photographs in public spaces, and no permission is required to take photographs in public places. However, on private property, the permission of the property owner, or in the case of a school the proprietor or the person with this delegated responsibility (normally the Head teacher) is required.
- Millbrook Junior School allows the photography when a performance/assembly has ended by the invited parent/carer/relative, providing the parent/carer/relative agrees to use the image only for private and domestic purposes. However, photos are to be of their own child only.
- Millbrook Junior School requires that all local press and media organisations have been informed that Millbrook Junior School does not wish identifying information to be published with photographs of its pupils taken at local and regional events.
- School should store images which are defined as "personal data", securely, in line with the terms of the Data Protection Act. Secure storage can be defined as an area on a school network which requires a secure username and password to access, or an encrypted data storage device, or a cloud storage solution access by a username and password over an SSL (encrypted) connection.
- Teachers are not to use their own cameras. Teachers should not store copies of such images on their own computers or storage devices, and images should be deleted from staff cameras or camera storage devices once transferred to a school secure storage.

Personal information on the school website:

- Staff photos and names are published on the school website
- Pupils names (first name and initial of surname) are referenced in newsletters which are available to download from the school website
- Photos of some children are published on the school website
- No pupils have their surnames published on the school website.

How to deal with Online Safety incidents – action to take:

In the first instance, staff should complete a concerns form (Appendix 8). Guidance for dealing with Online Safety issues found in Appendix 12. If illegal material is found on the network, or log evidence to suggest that illegal material has been accessed

- If the illegal material image is (or is suspected to be) a:
    - Child sexual abuse images hosted anywhere in the world
    - A non-photographic child sexual abuse images hosted in the UK
    - Or a criminally obscene adult content hosted in the UK
- Report to Head and/or Chair of Governors and report to the IWF - www.iwf.org.uk/report. Contact local police. In all instances, follow school's safeguarding procedures if a child protection incident is suspected, do not copy, archive, forward, send or print out the image – leave it in situ, and if in doubt seek advice from the IWF or your local police.
- If there is illegal material which you are unable to remove which involves Grooming, or suspected child abuse via the Internet
  Call your local police. Also contact CEOP www.ceop.police.uk/safety-centre/ who have an excellent record for removing such material quickly.

Appendix 1 Ofsted Inspection Guidance

Taken from School Inspection Handbook, Ofsted
Updated 27th August 2021

Under the Personal Development section point 244, the following statements relate to Online Safety:

- enabling pupils to recognise online and offline risks to their well-being – for example, risks from criminal and sexual exploitation, domestic abuse, female genital mutilation, forced marriage, substance misuse, gang activity, radicalisation and extremism – and making them aware of the support available to them
- enabling pupils to recognise the dangers of inappropriate use of mobile technology and social media

Under the Behaviour and Attitudes section point 228, the following statements relate to Online Safety:

- an environment in which pupils feel safe, and in which bullying, discrimination and peer-on-peer abuse – online or offline – are not accepted and are dealt with quickly, consistently and effectively whenever they occur

Under the Safeguarding section point 292, the following statements relate to Online Safety:

- always act in the best interests of children, pupils and students to protect them online and offline, including when they are receiving remote education or self isolating due to COVID-19

Previously, the following statements are from the Outstanding judgements.

- Pupils work hard with the school to prevent all forms of bullying, including online bullying and prejudice-based bullying.
- Pupils have an excellent understanding of how to stay safe online and of the dangers of inappropriate use of mobile technology and social networking sites.

Ofsted have previously defined e-safety thus (in their previous 'Inspecting e-safety in schools' briefings):

- 'In the context of an inspection, e-safety may be described as the school's ability to protect and educate pupils and staff in their use of technology and to have the appropriate mechanisms to intervene and support any incident where appropriate.

Appendix 3 – Job Description for Online Safety Officer

- Acting as a named point of contact on all online safety issues and liaising with other members of staff as appropriate.
- Keeping up-to-date with current research, legislation and trends. This may include accessing appropriate training and using a range of approaches to enable them to understand the role of new technology as part of modern British society and the wider safeguarding agenda.
- Ensuring that the setting participates in local and national events to promote positive online behaviour, e.g. Safer Internet Day.
- Ensuring that online safety is promoted to parents and carers and the wider community through a variety of channels and approaches.
- Maintaining an online safety incident/action log to record incidents and actions taken as part of the schools safeguarding recording structures and mechanisms.
- To monitor the delivery and impact of the online safety policy
- To monitor log of reported online safety incidents to inform future areas of teaching/learning/training.
- Monitoring and reporting on online safety issues to the school management team, Governing Body and other agencies as appropriate
- Liaising with the local authority and other local and national bodies as appropriate.

Appendix 6 - Filtering Guidance

Taken from: **https://www.saferinternet.org.uk/advice-centre/teachers-and-school-staff/appropriate-filtering-and-monitoring/appropriate-filtering**

Guide for education settings and filtering providers about establishing 'appropriate levels of filtering'

Schools in England (and Wales) are required **"to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering"**[1]. Furthermore, the Department for Education's statutory guidance **'Keeping Children Safe in Education'** obliges schools and colleges in England to "ensure appropriate filters and appropriate monitoring systems are in place" and they "should be doing all that they reasonably can to limit children's exposure to the above risks from the school's or college's IT system" however, schools will need to "be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding." **Ofsted concluded in 2010** that "Pupils in the schools that had 'managed' systems had better knowledge and understanding of how to stay safe than those in schools with 'locked down' systems. Pupils were more vulnerable overall when schools used locked down systems because they were not given enough opportunities to learn how to assess and manage risk for themselves."
Included within the Scottish Government national action plan on internet safety, schools in Scotland are expected to "have policies in place relating to the use of IT and to use filtering as a means of restricting access to harmful content."
The aim of this document is to help education settings (including Early years, schools and FE) and filtering providers comprehend what should be considered as 'appropriate filtering'.
It is important to recognise that no filtering systems can be 100% effective and need to be supported with good teaching and learning practice and effective supervision.

Illegal Online Content

In considering filtering providers or systems, schools should ensure that access to illegal content is blocked, specifically that the filtering providers:

- Are IWF members and block access to illegal Child Sexual Abuse Material (CSAM)
- Integrate the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'

Inappropriate Online Content

Recognising that no filter can guarantee to be 100% effective, schools should be satisfied that their filtering system manages the following content (and web search)

- Discrimination - Promotes the unjust or prejudicial treatment of people with protected characteristics of the Equality Act 2010
- Drugs / Substance abuse - displays or promotes the illegal use of drugs or substances

- Extremism - promotes terrorism and terrorist ideologies, violence or intolerance
- Malware / Hacking - promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content
- Pornography - displays sexual acts or explicit images
- Piracy and copyright theft - includes illegal provision of copyrighted material
- Self Harm - promotes or displays deliberate self harm (including suicide and eating disorders)
- Violence - displays or promotes the use of physical force intended to hurt or kill

This list should not be considered an exhaustive list and providers will be able to demonstrate how their system manages this content and many other aspects.
Regarding the retention of logfile (Internet history), schools should ensure clear and appropriate data retention policies and logfiles (Internet history) should include the identification of individuals and the duration to which all data is retained.
Providers should be clear how their system does not over block access so it does not lead to unreasonable restrictions.

Filtering System Features

Additionally, and in context of their safeguarding needs, schools should consider how their filtering system meets the following principles

- Age appropriate, differentiated filtering – includes the ability to vary filtering strength appropriate to age and role
- Circumvention – the extent and ability to identify and manage technologies and techniques used to circumvent the system, for example VPN, proxy services and DNS over HTTPS
- Control - has the ability and ease of use that allows schools to control the filter themselves to permit or deny access to specific content
- Contextual Content Filters – in addition to URL or IP based filtering, the extent to which (http and https) content is analysed as it is streamed to the user and blocked. For example, being able to contextually analyse text on a page and dynamically filter.
- Filtering Policy – the filtering provider publishes a rationale that details their approach to filtering with classification and categorisation as well as over blocking
- Group / Multi-site Management – the ability for deployment of central policy and central oversight or dashboard
- Identification - the filtering system should have the ability to identify users
- Mobile and App content – mobile and app content is often delivered in entirely different mechanisms from that delivered through a traditional web browser. To what extent does the filter system block inappropriate content via mobile and app technologies (beyond typical web browser delivered content)
- Multiple language support – the ability for the system to manage relevant languages
- Network level - filtering should be applied at 'network level' i.e., not reliant on any software on user devices whilst at school (recognising that device configuration/software may be required for filtering beyond the school infrastructure)
- Remote devices – with many children and staff working remotely, the ability for devices (school and/or personal) to receive school based filtering to a similar quality to that expected in school

- Reporting mechanism – the ability to report inappropriate content for access or blocking
- Reports – the system offers clear historical information on the websites visited by your users

Schools and Colleges should ensure that there is sufficient capability and capacity in those responsible for and those managing the filtering system. The **UK Safer Internet Centre Helpline** may be a source of support for schools looking for further advice in this regard.
Filtering systems are only ever a tool in helping to safeguard children when online and schools have an obligation to **"consider how children may be taught about safeguarding, including online, through teaching and learning opportunities, as part of providing a broad and balanced curriculum"**. To assist schools and colleges in shaping an effective curriculum, UK Safer Internet Centre has published **ProjectEVOLVE**
UK Safer Internet Centre recommends that those responsible for Schools and Colleges undertake (and document) an annual online safety risk assessment, assessing their online safety provision that would include filtering (and monitoring) provision. **The risk assessment should consider the risks that both children and staff** may encounter online, together with associated mitigating actions and activities.
A risk assessment module has been integrated in **360 degree safe**. Here schools can consider identify and record the risks posed by technology and the internet to their school, children, staff and parents.
To improve the appreciation of filtering services, SWGfL developed an **online utility** that enables users to discover capabilities of their filtering system.

Appendix 7 – Password Guidance:

- The use of network profiles which require the user to input a username and password is one way to enable the network manager to log network and Internet activity specific to a user, in order to fulfil Online Safety requirements.
- All staff to be aware that passwords should not be shared. Also at times, pupils might work in pairs or small groups. Staff to be aware that computers can be left logged on and as a result another user could cause an Online Safety incident which could be incorrectly attributed to the wrong person.
- There may be teaching and learning requirements which necessitate collaborative learning, shared access to group work, paired work or peer review tasks which require more than one user to access the same file, workstation or Internet browsing – rendering a user profile logging approach ineffective and unconstructive to teaching and learning.
- At times, it may be necessary to have users access websites with a site username password. These sites include (but not limited to): MyMaths, Linguascope, CLPE,

Appendix 8 – Social Media Guidance

Social Networking Guidance for Staff, Governors and Volunteers

Introduction

Social networking activities conducted online outside work, such as blogging (writing personal journals to publicly accessible internet pages), involvement in social networking sites such as Facebook or Twitter and posting material, images or comments on sites such as YouTube can have a negative impact on the school's reputation or image as well as having the potential to affect individual careers. In addition, Millbrook Junior School has a firm commitment to safeguarding children in all aspects of its work. This guidance has been written to set out the key principles and code of conduct and expectations of staff with respect to their responsibilities in connection with the use of social networking sites.

Key Principles

- Everyone at Millbrook Junior School has a responsibility to ensure that they protect the reputation of the school, and treat colleagues and members of the school with professionalism and respect.

- It is important to protect everyone at the school from allegations and misinterpretations that can arise from the use of social networking sites.

- Safeguarding children is a key responsibility of all members of staff and it is essential that everyone at Millbrook Junior School considers this and acts responsibly if they are using social networking sites out of school. Anyone working in the school either as a paid employee or volunteer, must not communicate with children (under the age of 21 or still in full time education, own family members exempt) via social networking.

- This guidance relates to social networking outside work. Blogging and accessing social networking sites at work is not permitted.

Aims

- To set out the key principles and code of conduct expected of all members of staff, governors and volunteers at Millbrook Junior School with respect to social networking.

- To further safeguard and protect children and staff.

Code of Conduct Millbrook Junior School – Social Networking

The following are **not considered acceptable** at Millbrook Junior School:

- The use of the school's name, logo, or any other published material without written prior permission from the Headteacher or Chair of Governors. This

applies to any published material including the internet or written documentation.

- The posting of any communication or images that links the school to any form of illegal conduct or which may damage the reputation of the school. This includes defamatory comments.

- The disclosure of any information that may harm the school, its pupils, staff or others associated with the school or images that could compromise the security of the school.

- The posting on social media/websites of any images of employees, children, governors or anyone directly connected with the school whilst engaged in school activities.

In addition to the above everyone at Millbrook Junior School must ensure that they:

- Comply with the Bullying and Harassment Policy and must not make any derogatory, defamatory, rude, threatening or inappropriate comments about the school, or anyone at, or connected with the school.

- Use social networking sites responsibly and ensure that either their personal/professional reputation, or the school's reputation is compromised by inappropriate postings.

- Are aware of the potential of on-line identity fraud and to be cautious when giving out personal information about themselves which may compromise their personal safety and security.

Potential and Actual Breaches of the Code of Conduct

In instances where there has been a breach of the above Code of Conduct, the following will apply:

- Any breaches of this guidance will be fully investigated. Where it is found that there has been a breach of the guidance, it may result in action being taken under the Disciplinary Procedure.

- The Governing Body will take appropriate action in order to protect the school's reputation and that of its staff, parents, governors, children and anyone else directly linked to the school.

Monitoring and Evaluation

- This guidance will be periodically reviewed at Millbrook Junior School as part of their programme of reviews.

Appendix 8a School Social Media Account

We recognise and embrace the numerous benefits and opportunities that various forms of social media can currently offer. While school employees are encouraged to engage, collaborate and innovate through social media, they should also be aware that there are some associated risks, especially around issues of safeguarding, bullying and personal reputation.

Definition of social media

Social media is a broad term for any kind of online platform which enables people to directly interact with each other. It allows people to share information, ideas and views. Examples of social media include blogs, Facebook, LinkedIn, Twitter, Google+, Instagram, Myspace, Flickr and YouTube.

The school's official social media presence: Facebook

The school has an official Facebook account managed by two members of staff. The current purposes and protocols relating to this account are as follows:

- The Facebook account is to be used:
    - to share and celebrate school activities and events;
    - (occasionally) to communicate important and urgent information to parents (along with other modes of communication).
- The Facebook page can be accessed on the Home page of the school website.
- Posts are only made by the nominated account managers.
- Account managers:
    - store account details and passwords securely;
    - must declare who they are in social media posts or accounts (anonymous posts are discouraged in relation to school activity);
    - regularly review the account and responses to posts;
    - regular monitoring and intervention is essential in case a situation arises where bullying or any other inappropriate behaviour arises on a school social media account;
    - should consider the copyright of the content they are sharing and, where necessary, should seek permission from the copyright holder before sharing;
    - must ensure that their use of social media does not infringe upon relevant data protection laws, or breach confidentiality;
    - should block, report or delete other users or their comments/posts and should inform the audience exactly why the action was taken, if a conversation turns and becomes offensive or unacceptable;
    - should exercise their professional judgement about whether an image is appropriate to share on school social media accounts.

- Any comments on the account that cause concern are removed immediately and the information passed on to the Headteacher.
- Any positive and supportive comments posted by parents or members of the public in response to posts are shared with the Headteacher.
- The tone of posts on the school Facebook page should always be *engaging, conversational, informative, friendly and respectful.*
- Permission to use any photos or video recordings is sought from parents / carers, in line with the school's digital and video images policy (GDPR). If anyone, for any reason, asks not to be filmed or photographed, then their wishes should be respected.
- No full names of children are included in messages or text relating to photos posted by the school account managers (occasionally children's initials may be used).
- In all photos posted on school social media accounts, pupils should be appropriately dressed, not be subject to ridicule and must not be on the list of children whose images should not be published.
- ***Professional communications*** are those made through official channels, posted on a school account or using the school name. All professional communications are within the scope of this policy.
- Parents / carers are encouraged to comment or post appropriately about the school. In the event of any offensive or inappropriate comments being made, the school will ask the parent/carer to remove the post and invite them to discuss the issues in person. If necessary, parents will be referred to the school's official complaints procedures.

Appendix 9 – Concerns Form

Online Safety Incident Report

This Event Report Form Compiled By:

Name of pupils involved:

Time and Date:

Staff informed with time and date (circle/name below):

Head Teacher

Online Safety Co-ordinator

Designated Safeguard Lead

Other

Nature of Concern (What happened? Please attach further sheet if required):

Who was involved: pupil/staff/parents?

Where did it occur: home, school?

Time and date of Incident:

Action taken:

Evidence preserved (Please attach copies of emails, images, or witness notes)

DSL to complete:
Other action

Other Officers Involved in Response:

LA Officer

Designated Officer LA

NCC Network Security Manager

Other

Follow up Action:

Evidence Collected (and where retained):

Reviewed:

Appendix 10 – AUP

Acceptable Use Policy – Staff, Governors and External Contractors

Our school promotes the positive use of technology in school and assists in developing pupil's knowledge and understanding of digital devices and the Internet. We ensure that our school IT network is robust and resilient and staff have a duty of care to safeguard pupils when using technology in school. Any misuse of technology by a pupil or member of staff must be reported to the Online Safety DSL (in their absence, report to DSL or Deputy DSL), so an investigation can take place.

This is the Acceptable User Policy (AUP) for our school. It highlights the do's/don'ts of using all technology in school and shows how we want staff to behave when using IT. The AUP covers the following legislation:

- Malicious Communications Act
- Data Protection Act 2018
- Computer Misuse Act 1990
- Communications Act 2003
- Sexual Offences Act 2003

Please read carefully and sign at the bottom to show you agree to these terms.

Using Technology in School

- I will only use school IT systems, external logins and email for school related purposes. Other use will be with the permission of SLT.
- I will monitor the use of IT in school and report any inappropriate use by pupils or staff to the Headteacher
- I will not search for, view, download, upload or transmit any material which could be considered illegal, offensive, extremist defamatory or copyright infringing.

Security, Passwords & Copyright

- I will not divulge any school related passwords and I will comply with school Password Guidance (Appendix 7). With permission from the Head (in their absence, the Deputy Head), there may be site username/passwords shared with all staff. This may include sites including, but not limited to, MyMaths, Linguascope.
- I will use school email systems for school related communications. I will not use personal accounts for school business.
- I will ensure that personal data is stored securely and in line with GDPR and the Data Protection Act. I will follow school guidance (Appendix 7 and Appendix 16) with regard to external logins, encrypted data and not storing school material on personal IT equipment unless stated otherwise. If using personal mobile device, written permission must be sort from Head Teacher (or Deputy Head in the absence of the Head). The school will provide a memory card for recording devices to enable images/recordings to be saved to. The Head or Deputy will then check personal device to ensure no images

are stored locally and will sign to confirm they have checked. See Appendix 16 for form.

- I will not install software onto the network or mobile devices unless permission sort by the Network Manager or IT support staff. These requests will be emailed to School Business Manager (currently Rachel Gibbs) to inform technical staff. However, if pre-installed software requires an update, these can be actioned without permission.

Social Media

- I must maintain my professionalism at all times when using personal social media and not bring the school or my profession into disrepute by posting unsuitable comments or media when using these sites.
- I must not use social media tools to communicate with current or former pupils under the age of 18 (family members exempt).

Mobile Technologies

- I will ensure that my mobile phone and any other personally-owned device is switched off or switched to 'silent' mode when I have directed time with pupils and stored in class safe/lockers. I will only make or receive calls in non-pupil places e.g. staffroom, workroom
- I will not contact any parents or pupils on my personally-owned device for school business.
- In line with the Use of Personal Mobile Devices Guidance guidance (Appendix 16), I will ensure that all school data on personal devices is password protected

Online Professionalism

- I am awarethat all network and Internet activity is logged and that the Deputy Head, Online Safety DSL and IT Technician can monitor the logs, and that they can be made available to SLT in the event of allegations ofmisconduct.
- I will not write or upload any defamatory, objectionable, copyright infringing or private material, including images and videos, of pupils, parents or staff on social media or websites. Images/videos of oneself (including tagged images/videos) must ensure that they do not, in any way, bring the school into disrepute.
- I will make sure that my Internet presence does not bring the teaching profession into disrepute and that I behave online in line with the Teacher Standards (2012).
- I will champion the school's online safety policy and be a role model for positive and responsible behaviour on the school network and the Internet.
- I will not give my home address, phone number, mobile number, personal social networking details or email address to pupils. Any personal communication with parents (i.e. birthday invites for children's parties) must be direct with parents not via pupil invites or in a sealed envelope labelled 'For attention of Parent/Carer of…' All other communication with parents should be done by authorised school contact channels.
- Photographs of staff, pupils and any other members of the school community will not be used outside of the internal school ITnetwork unless written

permission has been granted by the subject of the photograph or their parent/guardian. I will ask the permission of the Head Teacher prior to taking any photographs. No external photographs to be taken during school visits.

- I will ensure that any device I have logged onto has been locked when I am away from the device

Acceptable Use Policy

Signed:_____

Name:_____

Date:_____

Acceptable Use Policy Agreement - Pupil

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers / tablets
- I will only use activities that a teacher or suitable adult has told or allowed me to use
- I will take care of the computer and other equipment
- I will not tell anyone else my password.
- If someone finds out my password, I will tell my teacher so it can be changed
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong
- I will tell a teacher or suitable adult if I see something that upsets me on the screen
- I know that if I break the rules I might not be allowed to use a computer or chrome book.
- If I bring a mobile device to school, I will switch it off and give it straight to my teacher to lock in the classroom safe.
- I will not bring a smart watch, which allows recording or messaging, to school.

Name of Pupil: .....

Group / Class: .....

Signed: .....

Date: .....

Acceptable Use Agreement - Parent / Carer

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies provide powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- Millbrook Junior School systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that parents and carers are aware of the importance of online safety and are involved in the education and guidance of young people with regard to their on-line behaviour.
- Parents do not post negative comments about the school on social media sites and address any concerns you have directly with the school.

Millbrook Junior School will ensure to ensure that pupils will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users. A copy of the Student / Pupil Acceptable Use Policy is attached to this permission form, so that parents / carers will be aware of the school expectations of the young people in their care.
Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

Parent / Carer Permission Form

Parent / Carers Name:.....

Student / Pupil Name:.....

As the parent / carer of the above pupils, I give permission for my son / daughter to have access to the internet and to ICT systems at school.

Appendix 11 – Online Safety and the Law:

Computer Misuse Act 1990
Data Protection Act 2018
Freedom of Information Act 2000
Communications Act 2003
Protection from Harassment Act 1997
Regulation of Investigatory Powers Act 2000
Copyright, Designs and Patents Act 1988
Racial and Religious Hatred Act 2006
Protection of Children Act 1978
Sexual Offences Act 2003
The Education and Inspections Act 2006 (Head teachers have the power "to such an extent as is reasonable" to regulate the conduct of pupils off site. Also, staff can confiscate mobile phones if they cause disturbance in class breach the school behaviour policy.)

Copyright infringement and DMCA:
If a website is hosted in the USA, or operates under US law, then the Digital Millennium Copyright Act 1998 will apply for copyright infringement. This is very useful when seeking to remove photographs and other material which has been copied onto site such as Facebook and Twitter.

Duty of care and 'in loco parentis':
Schools have a 'duty of care' to pupils, and as such act "in loco parentis." Under the Children Act 1989 (updated 2004), this enables schools to remove personal information, cyber bullying and comments relating to school pupils as if they were the child's parent. Facebook in particular has provision for using 'in loco parentis' when reporting cyber bullying. This is relevant to all schools, but especially to boarding and residential schools.

Appendix 12- Dealing with Pupil Online Safety Incidents

Indicative sanctions for pupils and/or staff:
When an incident occurs, ALWAYS fill in Online Safety Incident form and give to Online Safety Officer. The Online Safety Officer will support and advise next steps. This may include (but not limited to):

- Class teacher speaking to pupils and/or parent/carer
- The Online Safety Officer speaking to the parent/carer

Illegal activities:

- The Head Teacher or delegated SLT with responsibility for pupil behaviour will deal with the matter.
- The Police and IWF/CEOP should be contacted. Child Protection procedures take precedence over AUPs if CP is a factor.
- The Network Manager, School IT Support or external IT contractor (if outside filtering services are used, for example) should be contacted to obtain further evidence.

Going on the inappropriate websites and searching inappropriate material:

- The class teacher will deal with the matter and write up an incident report to submit to the Online Safety Officer. The Online Safety Officer will then investigate and decide on course of action including sanctions. This may include speaking to the child, parent/carers, Head/Deputy and/or external agencies i.e. Police.

Bypassing the school's filtering system:

- The class teacher will deal with the matter and write up an incident report to submit to the Online Safety Officer. The Online Safety Officer will then investigate and decide on course of action including sanctions. This may include class teacher/Online Safety Officer speaking to the child, parent/carers and Head/Deputy.
- The Network Manager/School IT Support will be informed to identify how to stop the bypass from happening again.

Viewing pornographic material:

- The class teacher will deal with the matter and write up an incident report to submit to the Online Safety Officer. The Online Safety Officer will then investigate and decide on course of action including sanctions. This will include speaking to the child, parent/carers, Head/Deputy.
- The Police and IWF should be contacted if indecent material was uploaded or downloaded. CEOP should be contacted if grooming / sexting or unwanted sexual advances were involved.
- The Network Manager, School IT Support or external IT contractor (if outside filtering services are used, for example) should be contacted to obtain further evidence.

Using a mobile phone or other digital device in a lesson:

- The pupil will have their device removed. The class teacher will deal with the matter and parents will be informed.

Using social media (Snapchat, Instagram, Facebook or Twitter) or email in lesson time:

- The class teacher will deal with the matter and write up an incident report to submit to the Online Safety Officer. The Online Safety Officer will then investigate and decide on course of action including sanctions. This may include class teacher/Online Safety Officer speaking to the child, parent/carers and Head/Deputy.

Cyber bullying:

- Dealt with in accordance with Anti-Bullying policy
- Parents informed

Writing malicious comments about the school or bringing the school name into disrepute – whether in school time or not:

- If during lesson time, the class teacher will deal with the matter. They will write up an incident report to submit to the Online Safety Officer. The Online Safety Officer will then investigate and decide on course of action including sanctions.
- Parents will be informed.

Sharing usernames and passwords:

- Pupils reminded about the importance of not sharing passwords
- Pupil password to be changed

Trying to hack or hacking into another person's account, school databases, school website, school emails or online fraud using the school network:

- If during lesson time, the class teacher will deal with the matter and write up an incident report to submit to the Online Safety Officer. The Online Safety Officer will then investigate and decide on course of action including sanctions. This may include speaking to the child, parent/carers, Head/Deputy and/or external agencies i.e. Police.
- Depending on the severity of the incidence, the cybercrime unit, http://www.actionfraud.police.uk/or local police could be contacted.
- The Network Manager, School IT Support or external IT contractor (if outside filtering services are used, for example) should be contacted to obtain further evidence.
- Additionally, parent/carers will need to be informed.

Uploading or downloading unauthorised files using the school network:

- Pupils reminded about the dangers or uploading/downloading files
- Reported to Online Safety Officer using form
- Online Safety Officer to investigate and decide on course of action. This may include speaking to the child, parent/carers, Head/Deputy and/or external agencies i.e. Police.

Copyright infringement of text, software or media:

- Pupils reminded about the copyright rules
- Copyright infringement deleted
- If pupil continues to infringe copyright, class teacher to report to Online Safety Officer using form
- Online Safety Officer to investigate and decide on course of action. This may include speaking to the child, parent/carers, Head/Deputy and/or external agencies i.e. Police.

Appendix 13 Useful links to external organisations:

Information and support

There is a wealth of information available to support schools, colleges and parents to keep children safe online. The following list is not exhaustive but should provide a useful starting point:

Organisation/Resource	What it does/provides
Thinkuknow	NCA CEOPs advice on online safety
Disrespectnobody	Home Office advice on healthy relationships, including sexting and pornography
UK safer internet centre	Contains a specialist helpline for UK schools and colleges
swgfl	Includes a template for setting out online safety policies
internet matters	Help for parents on how to keep their children safe online
parentzone	Help for parents on how to keep their children safe online
pshe association	Guidance and useful teaching resources covering online safety issues including pornography and the sharing of sexual images
educateagainsthate	Practical advice for parents, teachers and governors on protecting children from extremism and radicalisation.
the use of social media for online radicalisation	A briefing note for schools on how social media is used to encourage travel to Syria and Iraq
UKCIS	The UK Council for Internet Safety's website provides: • Sexting advice • Online safety: Questions for Governing Bodies • Education for a connected world framework
NSPCC	NSPCC advice for schools and colleges
net-aware	NSPCC advice for parents
Commonsensemedia	Independent reviews, age ratings, & other information about all types of media for children and their parents
searching screening and confiscation	Guidance to schools on searching children in schools and confiscating items such as mobile phones
Lgfl	Advice and resources from the London Grid for Learning

The following links may help those who are developing or reviewing a school online safety policy:

UK Safer Internet Centre

Safer Internet Centre – https://www.saferinternet.org.uk/
South West Grid for Learning - https://swgfl.org.uk/products-services/online-safety/
Childnet – https://www.childnet.com/
Professionals Online Safety Helpline - http://www.saferinternet.org.uk/about/helpline
Internet Watch Foundation - https://www.iwf.org.uk/

CEOP

CEOP - http://ceop.police.uk/
ThinkUKnow - https://www.thinkuknow.co.uk/

Others

LGfL – Online Safety Resources
Kent – Online Safety Resources page
INSAFE / Better Internet for Kids - https://www.betterinternetforkids.eu/
UK Council for Internet Safety (UKCIS) formally UK Council for Child Internet Safety
https://www.gov.uk/government/news/new-council-for-internet-safety-in-the-uk
Netsmartz - https://www.netsmartzkids.org/

Tools for Schools

Online Safety BOOST – https://boost.swgfl.org.uk/
360 Degree Safe – Online Safety self-review tool – https://360safe.org.uk/
360Data – online data protection self review tool: www.360data.org.uk

Bullying / Online-bullying / Sexting / Sexual Harrassment

Enable – European Anti Bullying programme and resources (UK coordination / participation through SWGfL & Diana Awards) - http://enable.eun.org/
Scottish Anti-Bullying Service, Respectme - http://www.respectme.org.uk/
Scottish Government – Developing a positive whole school ethos and culture: relationships, learning and behaviour - http://www.scotland.gov.uk/Publications/2013/03/7388
DfE - Cyberbullying guidance - https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyberbullying_Advice_for_Headteachers_and_School_Staff_121114.pdf
Childnet – Cyberbullying guidance and practical PSHE toolkit: http://www.childnet.com/our-projects/cyberbullying-guidance-and-practical-toolkit
Childnet – Project deSHAME – Online Sexual Harrassment
UKSIC – Sexting Resources
Anti-Bullying Network – http://www.antibullying.net/cyberbullying1.htm
Ditch the Label – Online Bullying Charity
Diana Award – Anti-Bullying Campaign

Social Networking
Digizen – Social Networking

Social Media Guides - Safety Features on Social Networks

Curriculum
SWGfL Digital Literacy & Citizenship curriculum

Teach Today – www.teachtoday.eu/

Insafe - Education Resources

Mobile Devices / BYOD
Cloudlearn Report Effective practice for schools moving to end locking and blocking

Data Protection
360data - free questionnaire and data protection self review tool

ICO Guide for Organisations (general information about Data Protection)

ICO Guidance on Bring Your Own Device

ICO Guidance on Cloud Computing

ICO - Guidance we gave to schools - September 2012

IRMS - Information Management Toolkit for Schools

ICO Guidance on taking photos in schools

Dotkumo - Best practice guide to using photos

Professional Standards / Staff Training
DfE – Keeping Children Safe in Education

Childnet – School Pack for Online Safety Awareness

UK Safer Internet Centre Professionals Online Safety Helpline

Infrastructure / Technical Support
UKSIC – Appropriate Filtering and Monitoring

Somerset - Questions for Technical Support

NEN – Advice and Guidance Notes

Working with parents and carers
SWGfL Digital Literacy & Citizenship curriculum

Online Safety BOOST Presentations - parent's presentation

Vodafone Digital Parents Magazine

Childnet Webpages for Parents & Carers
Get Safe Online - resources for parents
Teach Today
Cerebra - Learning Disabilities, Autism and Internet Safety - a Parents' Guide

Research

Ofcom –Media Literacy Research

Appendix 14 – Online Safety Coverage

Particular behaviour which will be highlighted might include:

- Explaining why harmful or abusive images on the Internet might be inappropriate or illegal.
- Explaining why accessing age inappropriate, explicit, pornographic or otherwise unsuitable or illegal videos is harmful and potentially unsafe.
- Explaining how accessing and / or sharing other people's personal information or photographs might be inappropriate or illegal.
- Youth Produced Sexual Imagery (YPSI) and online radicalisation.
- Teaching why certain behaviour on the Internet can post an unacceptable level of risk, including talking to strangers on social networking; how to spot an unsafe situation before it escalates, and how illegal practices such as grooming can develop.
- Exploring in depth how cyber bullying occurs, how to avoid it, how to stop it, how to report it and how to deal with the consequences of it.
- Teaching pupils to assess the quality of information retrieved from the Internet, including recognising how reliable, accurate and relevant information is – particularly information obtained from search engines.
- Informing pupils and staff of copyright and plagiarism infringement laws, and potential consequences with regard to copying material for homework and coursework, copying photographs and images on social networking sites, copying material for using in teaching materials, downloading music, video, applications or other software files illegally.
- Encouraging responsible and effective digital literacy skills which extend beyond school and into the workplace.
- The medical and social effects of spending too much time on the Internet, games consoles or computers.

Appendix 15 – Protecting Data:

- Staff need to ensure that care is taken to ensure the safety and security of personal data regarding all of the school population, particularly, but not exclusively: pupils, parents and staff.
- Personal data should only be stored on secure devices. In other words, only computers, servers, file-servers, cloud space, or devices which require a user name and password to access the information. Furthermore, web based, extranet, E-learning or cloud services which include personal information need to run over an https:// protocol – ie an SSL secure encrypted connection.
- Accounts need to be logged off after use to prevent unauthorised access.
- By far the most effective way to safeguard personal data when off the school site it not to transfer personal information outside school systems.
- Any data taken off site is secured on encrypted memory sticks and password protected laptops.

Appendix 16 – Use of Personal Mobile Devices Guidance

- The following applies to personal mobile devices use by: pupils, parents, staff, other users which includes, but not limited to, mobile phones, tablets, smart watches, laptops.
- All teaching staff need to monitor pupil Internet and computer usage during lessons. Online Safety DSL will weekly monitor Filtering alerts.
- If using their personal device in school, they comply with the school's Use of Personal Mobile Devices guidance
- Staff must not use a Personal Hotspot to link their computer/ipad to the Internet
- Any member of staff or external contractor wishing to use a memory stick, must first get permission from the Headteacher or Deputy Head. If the device belongs to a member of staff, they must then scan the device before use. The member of staff must then alert the Online Safety Officer who will keep a log. If the device is from an external contractor, the device must be scanned by either the Technician or Online Safety Officer. The Online Safety Officer will then add this to the log.
- As referred to in the Safeguarding and Child Protection Policy,
- Information made available for parent/carers at Parent/Carer Evenings
- Our *Safeguarding and Child Protection Policy* is set out in a separate document. Section 15 refers to Mobile Phones and Cameras.
    - Staff are allowed to bring their personal phones to school for their own use, but will limit such use to non-contact time when pupils are not present. Staff members' personal phones will remain in their bags or cupboards during contact time with pupils.
    - Staff will not take pictures or recordings of pupils on their personal phones or cameras.
    - We will follow the General Data Protection Regulation and Data Protection Act 2018 when taking and storing photos and recordings for use in the school.
- Teachers and pupils are not to use their own cameras unless given express permission by headteacher and log completed on page 38. Teachers should not store copies of images on their own computers or storage devices, and images should be deleted from cameras or camera storage devices once transferred to a school secure storage. Pupils are not permitted to use phones/mobile devices or computers onsite.
- Millbrook Junior School provides wireless connectivity as a guest service and offers no guarantees that any use of the wireless connection is in any way secure or that any privacy can be protected when using this wireless connection.
- Millbrook Junior Schools' wireless network is entirely at the risk of the user and the school is not responsible for any loss of any information that may arise from the use of the wireless connection, or from any loss, injury or damage resulting from use of the wireless connection.
- Millbrook Junior Schools' networks are bound by the respective school's computer acceptable use policy. In signing that, you agree to the Use of Personal Devices guidance you are agreeing to all of the above cautions and policies as they pertain to non- school devices. Any visitors who are given access to the school's network will be asked to sign the AUP.
- Once on the wireless network, all users will have filtered internet access just as they would on a school owned device.

- Personal devices must not be used when pupils are present.
- Teachers shall make no attempts to circumvent the school's network security. This includes setting up proxies and downloading programs to bypass security
- Millbrook Junior School has the right to take action against anyone involved in incidents of inappropriate behaviour, that are covered in the Acceptable Use Policy or school Behaviour Policy, whether in school or out of school (examples would be cyber-bullying, use of images or personal information.
- Pupils who bring mobile devices into school, must immediately switch them off and hand them to their class teacher who will place them into their classroom safe. Mobile phones must remain off until they have left the school site.
- Staff must store their mobile devices in lockers/safes provided.

Log for using personal device to take images/recordings

Name	Date device to be used	Agreed by (name, role and signed)	Equipment used (school to provide memory card)	Number of photos taken	Equipment checked to ensure no images/ recordings stored locally	Signed by Head on return on memory card

Appendix 17 – Annex C: Online safety

(Copied from Keeping Children Safe in Education 2023)

Online safety

135. It is essential that children are safeguarded from potentially harmful and inappropriate online material. An effective whole school and college approach to online safety empowers a school or college to protect and educate pupils, students, and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate.
136. The breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas of risk: content: being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism. contact: being subjected to harmful online interaction with other users; for example: 37 UK Council for Internet Safety Education subgroup is made up of sector experts who collaborate to produce advice and guidance to support schools and colleges keep their children safe online. 38Public Health England: has now been replaced by the UK Health Security Agency and the Office for Health Improvement and Disparities (OHID), which is part of the Department of Health and Social Care, and by the UK Health Security Agency, however branding remains unchanged. 36 peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes. conduct: online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and nonconsensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying, and commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).
137. Governing bodies and proprietors should ensure online safety is a running and interrelated theme whilst devising and implementing their whole school or college approach to safeguarding and related policies and procedures. This will include considering how online safety is reflected as required in all relevant policies and considering online safety whilst planning the curriculum, any teacher training, the role and responsibilities of the designated safeguarding lead (and deputies) and any parental engagement.

Online safety policy
138. Online safety and the school or college's approach to it should be reflected in the child protection policy which, amongst other things, should include appropriate filtering and monitoring on school devices and school networks. Considering the 4Cs (above) will provide the basis of an effective online policy. The school or college should have a clear policy on the use of mobile and smart technology, which will also reflect the fact many children have unlimited and unrestricted access to the internet via mobile phone networks (i.e. 3G, 4G and 5G). This access means some children, whilst at school or college, sexually harass, bully, and control others via their mobile

and smart technology, share indecent images consensually and non-consensually (often via large chat groups) and view and share pornography and other harmful content. Schools and colleges should carefully consider how this is managed on their premises and reflect this in their mobile and smart technology policy and their child protection policy. Remote education
139. Guidance to support schools and colleges understand how to help keep pupils, students and staff safe whilst learning remotely can be found at Safeguarding and remote education - GOV.UK (www.gov.uk) and Providing remote education: guidance for schools - GOV.UK (www.gov.uk). The NSPCC also provides helpful advice - Undertaking remote teaching safely.
140. Schools and colleges are likely to be in regular contact with parents and carers. 37 Those communications should be used to reinforce the importance of children being safe online and parents and carers are likely to find it helpful to understand what systems schools and colleges use to filter and monitor online use. It will be especially important for parents and carers to be aware of what their children are being asked to do online, including the sites they will be asked to access and be clear who from the school or college (if anyone) their child is going to be interacting with online.

Filtering and monitoring
141. Whilst considering their responsibility to safeguard and promote the welfare of children and provide them with a safe environment in which to learn, governing bodies and proprietors should be doing all that they reasonably can to limit children's exposure to the above risks from the school's or college's IT system. As part of this process, governing bodies and proprietors should ensure their school or college has appropriate filtering and monitoring systems in place and regularly review their effectiveness. They should ensure that the leadership team and relevant staff have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when identified. Governing bodies and proprietors should consider the number of and age range of their children, those who are potentially at greater risk of harm and how often they access the IT system along with the proportionality of costs versus safeguarding risks.

142. The appropriateness of any filtering and monitoring systems are a matter for individual schools and colleges and will be informed in part, by the risk assessment required by the Prevent Duty39. To support schools and colleges to meet this duty, the Department for Education has published filtering and monitoring standards which set out that schools and colleges should:
• identify and assign roles and responsibilities to manage filtering and monitoring systems
• review filtering and monitoring provision at least annually
• block harmful and inappropriate content without unreasonably impacting teaching and learning
• have effective monitoring strategies in place that meet their safeguarding needs.

Governing bodies and proprietors should review the standards and discuss with IT staff 39 The Prevent duty Departmental advice for schools and childcare providers and Home Office Statutory guidance: Prevent duty guidance. 38 and service

providers what more needs to be done to support schools and colleges in meeting this standard. Additional guidance on "appropriate" filtering and monitoring can be found at: UK Safer Internet Centre: https://www.saferinternet.org.uk/advice-centre/teachers-and-schoolstaff/appropriate-filtering-and-monitoring. The UK Safer Internet Centre produced a series of webinars for teachers on behalf of the Department. These webinars were designed to inform and support schools with their filtering and monitoring responsibilities and can be assessed at Filtering and monitoring webinars available – UK Safer Internet Centre. South West Grid for Learning (swgfl.org.uk) has created a tool to check whether a school or college's filtering provider is signed up to relevant lists (CSA content, Sexual Content, Terrorist content, Your Internet Connection Blocks Child Abuse & Terrorist Content).

143. Support for schools when considering what to buy and how to buy it is available via the: schools' buying strategy with specific advice on procurement here: buying for schools. Information security and access management
144. Education settings are directly responsible for ensuring they have the appropriate level of security protection procedures in place in order to safeguard their systems, staff and learners and review the effectiveness of these procedures periodically to keep up with evolving cyber-crime technologies. Guidance on e-security is available from the National Education Network. In addition, schools and colleges should consider meeting the Cyber security standards for schools and colleges.GOV.UK. Broader guidance on cyber security including considerations for governors and trustees can be found at Cyber security training for school staff - NCSC.GOV.UK. Reviewing online safety
145. Technology, and risks and harms related to it, evolve, and change rapidly. Schools and colleges should consider carrying out an annual review of their approach to online safety, supported by an annual risk assessment that considers and reflects the risks their children face. A free online safety self-review tool for schools can be found via the 360 safe website or LGfL online safety audit.
146. UKCIS has published Online safety in schools and colleges: Questions from the governing board. The questions can be used to gain a basic understanding of the current approach to keeping children safe online; learn how to improve this approach where appropriate; and find out about tools which can be used to improve the approach. It has also published an Online Safety Audit Tool which helps mentors of trainee teachers and newly qualified teachers induct mentees and provide ongoing support, development and monitoring. 39
147. When reviewing online safety provision, the UKCIS external visitors guidance highlights a range of resources which can support educational settings to develop a whole school approach towards online safety.

Appendix 18 – Online Safety and GDPR

Adapted from www.opendium.com

The General Data Protection Regulation (GDPR), replaced the existing Data Protection Act on May 25th 2018. Schools have a number of online safeguarding obligations under the Prevent duty, and the more recent Keeping Children Safe in Education guidance that came into effect in 2016 (updated 2018) – See Appendix 17 for Annex C from Keeping Children Safe in Education 2018.

The internet filtering and reporting systems that allow schools to carry out these duties have to collect a large amount of personal data about the users in the form of internet traffic logs.

Filtering systems will use the collected data to profile the users in order to flag up concerning behaviour, or to automatically impose bans on their internet access. A side effect of collecting these data is that the school is now responsible for the handling of data which could reveal very sensitive details about an individual, such as their sexual orientation, political opinions and religious beliefs. Under GDPR, this data is considered "special categories of personal data" and are afforded stronger protections.

The regulations hold the school accountable for the security of data that have been collected by the filtering system, and the lawfulness of their use. The regulations promote data minimisation - avoiding keeping personal data for longer than it is needed. This should be taken into account when deciding upon a suitable retention period. Old data can either be erased or anonymised, since anonymous data is not regulated by GDPR.

Our data protection officer is Paul Stratford. Contact details available on Privacy Policy.

One of the most important parts of the regulations is the requirement to keep individuals informed. The school should formulate a privacy policy and make it available to everyone that uses the school's internet connection. The policy will need to contain:

- The identity and contact details of both the school itself and the school's data protection officer.
- The reason why the data is being collected and used.
- Why it is lawful for the data to be collected and used in this way.
- Information about any third parties that may have access to the data.
- On request, how long the data will be kept for.
- Information about any automated decisions which may be made.
- An explanation of an individual's rights.

For all information relating to the above can be found in the school's Privacy policy March 2018.

Appendix 19 – Questions from the Governing board – gov.uk publication

Online safety in schools and colleges: Questions from the Governing Board

UK COUNCIL FOR CHILD INTERNET SAFETY

1. Does the school/college have online safety and acceptable use policies in place? How does the school/college assess that they are clear, understood and respected by all children and staff?

Why this question?	The Department for Education's (DfE) 2016 Keeping Children Safe in Education (KCSIE) statutory guidance states that "Governing bodies and proprietors should ensure there are appropriate procedures in place…to safeguard and promote children's welfare…which should amongst other things include… acceptable use of technologies…and communications including the use of social media."[1] However, the 2015 Ofsted Inspection Data reported that 5% of schools didn't have an online safety policy.
What to look for?	■ Systematic and regular review of online safety policies, at least on an annual basis. ■ Evidence that online safety policies are freely and readily available (e.g. posters, school/ college website, staff handbooks, etc.). ■ Pupils, staff, parents and carers are aware of online safety rules and expectations.
What is good or outstanding practice?	■ Collaborative production and review of policies, for example, evidence of the active use of pupils' and parents views. ■ Evidence of monitoring and evaluation processes to ensure understanding of, and adherence to, online safety policies. ■ Linked to and a part of other policies, such as safeguarding policies.
When should you be concerned?	■ No or minimal online safety policies ■ Policy is generic and not relevant to the school / college / pupil's needs ■ No / irregular review of online safety policy ■ Policies exist but are not publicised to the school/ college body and / or are not known by staff and pupils.

2. What mechanisms does the school / college have in place to support pupils, staff and parents facing online safety issues?

Why this question?	South West Grid for Learning (SWGfL) concluded in their sexting surveys over time (2009-2014)[2] of 1,100 11–16 year olds that 74% would prefer to report issues to their friends rather than a 'trusted adult'. The 2015 Ofsted's Online Safety Inspection Data found that reporting is clearly the weakest area of school practice around online safety, with reporting being both poorly understood and inconsistent. Many pupils were unclear about how to report when things went wrong and when they needed support. Further, in September 2015, Ofsted stated that "Inspectors should investigate what the school or further education and skills provider does to educate pupils in online safety and how the provider or school deals with issues when they arise."[3] With regards to monitoring and filtering, the 2016 KCSIE statutory guidance states "As schools and colleges increasingly work online it is essential that children are safeguarded from potentially harmful and inappropriate online material. As such governing bodies and proprietors should ensure **appropriate filters and appropriate monitoring systems** are in place."
What to look for?	■ Online safety clearly recognised as a safeguarding issue within the roles and responsibilities of the school/ college Designated Safeguarding Leads (DSL) ■ Robust reporting channels which could be defined as: ➢ Well-defined, clearly understood and consistent reporting channels. ➢ Whole-school/college approach, in which reporting channels include teachers, parents and pupils. ➢ Multiple reporting routes for pupils and parents which they have confidence in. ■ Clearly articulated procedures for responding to different online risks (Sexting; Online Bullying; Online grooming etc.) ■ Regular review of monitoring and filtering provisions as part of safeguarding responsibilities e.g. Evidence of communication between technical staff and DSLs Links into other relevant policies and procedures e.g. complaints, allegations etc.
What is good or outstanding practice?	■ Online reporting mechanisms for students and parents. ■ All staff are aware of sources of support for online safety issues, such as the Professionals Online Safety Helpline. ■ Nominated members of staff with appropriate skills and responsibilities e.g. (DSL), trained and available to deal with the various risks related to online activity. ■ Planned and effective peer support strategies, e.g. reporting mechanisms / escalation processes supported by professionals and teachers. ■ Auditing of online behaviour and risks which provides base line information from the pupils about the levels and types of online issues prevalent in the school / college. ■ Regular evaluation of reporting channels and response procedures. ■ Online safety information / data highlighted within the Head Teacher's report to the governing board.

When should you be concerned?	■ No / inconsistent reporting channels. ■ No recording processes to enable the school/ college to identify and monitor concerns. ■ Pupils and parents unaware of reporting channels. ■ Reporting routes pupils and parents lack confidence in.

[1] P14.
[2] Sharing personal images and videos among young people, SWGfL & Plymouth University, 2009; http://www.swgfl.org.uk/Staying-Safe/Sexting-Survey.
[3] p15, Inspecting safeguarding in early years, education and skills settings, Ofsted, September 2015

3. How do you ensure that all staff receive appropriate online safety training that is relevant and regularly updated?

Why this question?	The SWGfL Online Safety Policy and Practice (2015) report found that over 50% of schools had carried out no online safety training for their staff. The 2015 Ofsted inspection data presented a stronger picture but training was still found to be inconsistent, and suggested that what senior leadership teams saw as training was not always seen as such by staff.
What to look for?	■ Training content which improves staff knowledge of, and expertise in, safe behaviours and appropriate use of technologies.[4] ■ Audit of the training needs of all staff. ■ At least annual training (in-service or online) for all staff. ■ Online safety training coordinated by recognised appropriate individual (e.g. DSL) or group with online safety responsibility
What is good or outstanding practice?	■ DSL has a **higher level of training**, **knowledge and expertise** on online safety issues, with clearly defined responsibilities related to online safety provision for the school / college community. ■ Expertise on online safety is developed across a pool of staff, to ensure transfer and sustainability of knowledge and training. ■ Online safety training clearly established within the school/ college's wider safeguarding training ■ Training content updated to reflect current research and advances in technology as well as local policy and procedures.
When should you be concerned?	■ No recognised individual / group for online safety or they lack appropriate training and authority ■ DSL lacking appropriate training and authority in online safety training. ■ No, little or out-of-date training for all staff ■ There are teaching and pastoral staff that have no online safety training. ■ Training on online safety which does not meet the needs of staff – with the aim of improving knowledge of, and expertise in, the safe and appropriate use of technologies. ■ Training based on outdated resources / materials. ■ Regular training (at least annual) is not undertaken. ■ Lack of clarity on who coordinates staff training.

[4] This is a specific recommendation for schools from Ofsted's 2010 landmark report, The safe use of new technologies, p6.

4. Describe how your school/college educates children and young people to build knowledge, skills and confidence when it comes to online safety? How do you assess its effectiveness?

Why this question?	A key recommendation in the Byron review (2008)[5] was building the resilience of children to online issues through progressive and appropriate education. In response to the Byron Review, Ofsted stated in their 2010 report The safe use of new technologies that schools should "provide an age-related, comprehensive curriculum for e-safety which enables pupils to become safe and responsible users of new technologies".[6] In September 2015, Ofsted stated that "Inspectors should investigate what the school or further education and skills provider does to educate pupils in online safety ..."[7] With specific reference to the governing board, the 2016 KCSIE statutory guidance states "Governing bodies and proprietors should ensure children are taught about safeguarding, including online, through teaching and learning opportunities, as part of providing a broad and balanced curriculum. This may include covering relevant issues through personal, social, health and economic education (PSHE), tutorials (in FE colleges) and / or – for maintained schools and colleges – through sex and relationship education (SRE)".[8]
What to look for?	■ **Planned** online safety education programme which is: ➢ Taught across all age groups, and progresses as pupils grow and develop. ➢ Regular as opposed to a one-off online safety sessions. ➢ Incorporates / make use of relevant national initiatives and opportunities such as Safer Internet Day and Anti-bullying week. ■ Use of appropriate and up-to-date **resources.** ■ Resources from external providers may be used appropriately to support and compliment internal programmes. ■ Accessible to pupils at different ages and abilities, such as pupils with Special Educational Needs and Disabilities (SEND), or those with English as an additional language. ■ Pupils are able to **recall, explain and actively use** online safety education. ■ Teachers have access to appropriate training, to ensure teaching on online safety is undertaken by trained staff.
What is good or outstanding practice?	■ **Online safety is embedded throughout the school/college curriculum.** This means that the knowledge, skills and confidence of pupils, on issues related to online safety, are planned into all relevant school lessons such as PSHE education, as well as Sex and Relationships Education and computing. ■ **Regular review** of online safety sessions to ensure their relevance.
When should you be concerned?	■ Ad-hoc / **one-off sessions** on online safety, such as sessions only delivered through assemblies. ■ Content used is inaccurate, irrelevant, out of date and / or inappropriate for the age of the child. ■ Sole reliance on external providers to provide online safety education to learners. ■ No means to evaluate the effectiveness of education tools, and assess pupils' learning in this area.

[5] Safer children in a digital world: the report of the Byron Review (PP/D16(7578)/03/08), DCSF and DCMS, 2008.
[6] p6,The Safe Use of New Technologies, Ofsted, 2010
[7] p15, Inspecting safeguarding in early years, education and skills settings, Ofsted, September 2015.
[8] P17/18.

5. How does the school/college educate parents and the whole school/college community with online safety?

Why this question?	A key finding from the Ofcom Children's Media Lives reports (2016)[9] is that many parents lack confidence in their ability to support their children in dealing with online risks, due to lack of confidence in using technology and digital media. Parent Zone's 2014 report[10] also found "Supporting and enabling parenting has more of a positive impact on resilience than parental strategies to restrict or monitor internet use". Accordingly, Ofsted's 2010 report states schools should "work closely with all families to help them ensure that their children use new technologies safely and responsibly both at home and school".[11]
What to look for?	■ Regular communication, awareness-raising and engagement on online safety issues, such as through the school/college's communications outlets, such as the school website and newsletters. ■ Regular opportunities for engagement with parents on online safety issues.
What is good or outstanding practice?	■ Interactive engagement with parents, with the aim of building skills and confidence in dealing with online risks, as well as general awareness on online safety issues. ■ Regular and relevant online safety resources and sessions offered to parents. Relevant resources will tackle key online risks and behaviours displayed by pupils at different ages in the school/college. ■ Evidence of pupils educating parents. ■ Online safety information available in a variety of formats which considers the needs of different parents, such as those with English as an additional language.
When should you be concerned?	■ No / minimal awareness-raising on online safety issues. ■ No online safety engagement with parents. ■ Recurrent problem behaviours amongst pupils (such as younger pupils playing games aimed towards older adolescents and adults).

[9] P10.
[10] P4, "A Shared Responsibility: Building Children's Online Resilience", Parentzone, 2014.
[11] P6.

Appendix 1: Where to go for more support

1. Does the school/college have online safety and acceptable use policies in place? How does the school/college assess that they are clear, understood and respected by all children and staff?

- Policy Templates, Guidance documents, and Acceptable Use Policy Templates for Education Settings, Kent County Council: http://www.kelsi.org.uk/support-for-children-and-young-people/child-protection-and-safeguarding/e-safety
- School Online Safety Policy Templates by the South West grid for Learning (SWGfl). SWGfl

is an educational charitable trust: http://swgfl.org.uk/products-services/esafety/resources/online-safety-policy-templates

- London Grid for Learning (LGfL): http://onlinesafety.lgfl.net
- 'SWGFL 360 degree safe' audit tool which enables schools to evaluate their own online safety provision: https://360safe.org.uk/

2. What mechanisms does the school/college have in place to support pupils, staff and parents facing online safety issues?

- Advice for practitioners (including school staff) provides detailed information as to what to do if there are concerns a child is being abused, by the Department of Education, UK Government: https://www.gov.uk/government/publications/what-to-do-if-youre-worried- a-child-is-being-abused--2

- Appropriate filtering and monitoring guides for schools and education settings, by the UK Safer Internet Centre: http://www.saferinternet.org.uk/advice-and-resources/teachers-and-professionals/appropriate-filtering-and-monitoring

- CEOP Safety Centre - for help, advice or to report an incident: http://www.ceop.police.uk/

- The Professionals Online Safety Helpline, by the UK Safer Internet Centre: http://www.saferinternet.org.uk/about/helpline

- Access your local policies and procedures - some regional broadband consortia, local authorities and/or local safeguarding children's boards may have specific policies and procedures for responding to some online safety risks

3. How do you ensure that all staff receive appropriate online safety training that is relevant and regularly updated?

There is plenty of training material and courses provided by:

- CEOP offers one day training for professionals (paid Ambassador training) on online safety.

- UK Safer Internet Centre advice and resources for teachers and professionals: http://www.saferinternet.org.uk/advice-and-resources/teachers-and-professionals and Online Safety Briefings from young people: www.onlinesafetylive.com

- Childnet's Professional resources: http://www.childnet.com/teachers-and-professionals

- Keeping Children Safe Online by the children's charity NSPCC and CEOP, is an online introductory safeguarding course for anyone who works with children: https://www.nspcc.org.uk/what-you-can-do/get-expert-training/keeping-children-safe-online-course/

- Access any local support available- some regional broadband consortia, local authorities or local safeguarding children's boards offer online safety training for professionals

4. Describe how your school/college educates children and young people to build knowledge, skills and confidence when it comes to online safety? How do you assess its effectiveness?

There are a number of resources for children and young people developed by organisations who specialise in children's online safety:

- CEOP's online safety education programme called Thinkuknow: http://www.thinkuknow.co.uk/

- Childnet (a non-for-profit organisation working in online safety): http://www.childnet.com/resources

- UK Safer Internet Centre, (a coordinated partnerships of SWGfL, the Internet Watch Foundation and Childnet): https://www.saferinternet.org.uk/

- SWGfL and Common Sense Media, which includes curriculum mapping: http://swgfl.org.uk

5. How does the school/college educate parents and the whole school/college community with online safety?

- Parent Zone, a not-for-profit organisation, offers Parents information to help understand the digital world and raise resilient children. They also offer training for teachers on how to engage parents: http://parentzone.org.uk/
- Parent and Carer support from the UK Safer Internet Centre: http://www.saferinternet.org.uk/advice-and-resources/parents-and-carers
- Childnet, provides information and advice for parents and carer, including a printable sheet available in 12 languages: http://www.childnet.com/resources/supporting-young-people-online
- Vodafone's Digital Parenting resources: http://www.vodafonedigitalparenting.co.uk
- Netware by NSPCC and O2, offers a guide to social networks for parents. https://www.net-aware.org.uk
- Share Aware by NSPCC and O2, offers advice to parents about the internet: https://www.nspcc.org.uk/keeping-children-safe/
- Parentinfo by CEOP and Parent Zone provides high quality information to parents and carers: http://parentinfo.org
- Parents section of CEOP's Thinkuknow website. https://www.thinkuknow.co.uk/parents/
- Engaging parents with online safety by Kent Country Council: https://www.kelsi.org.uk/__data/assets/pdf_file/0010/73837/Engaging-Families-in-Online-Safety.pdf