Policy Title	Online Safety Policy
Person(s) responsible for reviewing/updating the Policy	Chantal Warwick
Approval Required By	SLT
Review Cycle	Annually
Last Review Date	July 2024
Next Review Date	July 2025
Comments	In November 2019 we started using the 360Safe Online Safety Review Tool. The 360-degree safe tool allows schools to review their online safety provision, benchmark it against good practice and other schools, produce action plans and access good practice resources. We use the SWGfL Template as recommended in the 360Safe Review resources and shared by WSCC. The process involved carefully reviewing the previous policy contents and adding in further detail using the SWGfL template. By the time the Policy was completed we found ourselves in Lockdown and it was imperative to ensure that our students, now working remotely, had the latest guidance and policy to support them. The next step, moving forward with the 360Safe Review tool to implement procedures and training to promote our existing status.

Scope (or Who is Governed by this Policy)	Students, Teachers, Leadership Groups
Links to other Policies or Procedures or Documents *(Including their location – physical or electronic)*	Assessment, Reporting, Recording Policy Remote Teaching and Learning Policy
Policy document location	Whole School Resources Millais online-safety-policy-with-page numbers.docx
Where this Policy is published	Website : https://www.millais.org.uk/app/os#!/school-policies/online-policy

Millais School

Online Safety Policy

Contents

Introduction

SWGfL/UK Safer Internet Centre

The Southwest Grid for Learning Trust is an educational trust with an international reputation for supporting schools with online safety.

SWGfL, along with partners Child net and IWF, launched the UK Safer Internet Centre (UKSIC) in January 2011 as part of the European Commission's Safer Internet Programme. The Safer Internet Centre is, for example, responsible for the organisation of Safer Internet Day each February. More information about UKSIC services and resources can be found on the website: www.saferinternet.org.uk. SWGfL is a founding member of UKCIS (UK Council for Internet Safety). It has contributed to conferences across the world and has worked with government and other agencies in many countries. More information about its wide-ranging online safety services for schools can be found on the SWGfL website – swgfl.org.uk

360 Degree Safe Online Safety Self Review Tool

360 degree safe is an online, interactive self-review tool which allows schools/academies to review their online safety policy and practice.

tool provides an "improvement action" describing how the school might move from that level to the next. Users can immediately compare their levels to the average levels of all the schools/academies using the tool and to the Online Safety Mark benchmark levels. There is a range of reports that they can use internally or with consultants.

The tool suggests possible sources of evidence, provides additional resources/good practice guidance and collates the school's action plan for improvement.

Schools that reach required benchmark levels can apply for assessment for the Online Safety Mark, involving a half day visit from an accredited assessor who validates the school's self-review. More information about the Online Safety Mark can be found in the Accreditation section of the 360 tool.

Online Safety BOOST packages bring you extra empowerment and support to deal with your online safety challenges, official or otherwise. It comprises a toolkit of apps, services, tools and resources that all go to save time, equip your school to be more sensitive to, and better manage, online safety situations and issues.

Development, Monitoring & Review of this Policy.

This Online Safety policy has been developed by the Millais School Online Safety Committee made up of:

- Headteacher
- Online Safety Coordinator : Chantal Warwick [Assistant Headteacher]
- DSL : Mike Sutton [Deputy Headteacher]
- ICT Network Manager : Rob Dearsley
- Staff – including Teachers, Support Staff, Technical staff.
- Governors : ** TBC **
- Parents and Carers

Consultation with the whole school community has taken place through a range of formal and informal meetings.

Schedule for Development, Monitoring & Review

This Online Safety policy was approved by the Governing Body on:	June 2020
The implementation of this Online Safety policy will be monitored by the:	Online Safety Coordinator Chantal Warwick
Monitoring will take place at regular intervals:	Each February
The Governing Body will receive a report on the implementation of the Online Safety Policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	Each May
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	June 2025
Should serious online safety incidents take place, the following external persons / agencies should be informed:	PC Sally Scott DS211 **Prevention Youth Officer** **Horsham, Worthing and Adur** **Prevention Team** **West Sussex Division**

The school will monitor the impact of the policy using: Logs of reported incidents.

- Monitoring logs of internet activity (including sites visited) / filtering.
- Internal monitoring data for network activity
- Surveys of students, parents / carers, staff

Scope of the Policy

This policy applies to all members of the school community (including staff, students, volunteers, parents / carers, visitors, community users) who have access to and are users of school digital technology systems, both in and out of the school.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online-bullying or other Online Safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix for template policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate Online Safety behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the school:

Governors / Board of Directors

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Online Safety Governor The role of the Online Safety Governor will include:

- regular meetings with the Online Safety Lead (DSL)
- attendance at Online Safety Group meetings
- regular monitoring of online safety incident logs

- regular monitoring of filtering / change control logs
- reporting to relevant Governors / Committee / meeting

Headteacher and Senior Leaders

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day-to-day responsibility for online safety will be delegated to the Online Safety Lead.
- The Headteacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (See flow chart on dealing with online safety incidents – included in a later section – "Responding to incidents of misuse" and relevant Local disciplinary procedures).
- The Headteacher is responsible for ensuring that the Online Safety Lead (DSL) and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Headteacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- 12.2 Filters and monitoring from the Safeguarding Policy states:
  Millais School will do all we reasonably can to limit children's exposure to the risks outlined above from the school's IT system. We will ensure our school has the appropriate filters and monitoring systems in place. We will consider our prevent duties when identifying what filters and monitoring to adopt. We will also consider the advice given by the .UK Safer Internet Centre, found here.
  Our school will also consider further guidance contained within Keeping Children Safe in Education 2019, page 93, in respect of procurement decisions regarding what system to adopt.
  The school currently employs the services of 'Smoothwall' and safeguarding breaches or concerns in relation to online behaviour, bullying, radicalisation and safety are flagged with the DSL team for investigation. Follow up conversations are had within 24 hours and ideally on the day of alert. In serious cases Smoothwall will contact the DSL by telephone for immediate action.
- The Senior Leadership Team will receive regular monitoring reports from the Online Safety Lead (DSL).

Online Safety Lead (CLW)

- plays an integral role on the Online Safety Group
- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents.
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provides training and advice for staff.

- liaises with the Local Authority.
- liaises with school technical staff.
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments,
- meets regularly with Online Safety Governor to discuss current issues, review incident logs and filtering / change control logs.
- attends relevant meeting / committee of Governors.
- reports regularly to Senior Leadership Team
- Designated Safeguarding Lead should be trained in Online Safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:
    - sharing of personal data
    - access to illegal / inappropriate materials
    - inappropriate on-line contact with adults / strangers
    - potential or actual incidents of grooming
    - online-bullying

Network Manager

The Network Manager is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required online safety technical requirements and any Local Authority Online Safety Policy / Guidance that may apply.
- that users may only access the networks and devices through a properly enforced authentication policy including, where possible, MfA.
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the network / internet / Learning Platform / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher; Online Safety Lead for investigation / action / sanction.
- that monitoring software / systems are implemented and updated as agreed in school policies.

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up-to-date awareness of online safety matters and of the current school Online Safety Policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem to the Headteacher and Online Safety Lead for investigation / action / sanction.
- all digital communications with students / parents / carers should be on a professional level and only carried out using official school systems.
- online safety issues are embedded in all aspects of the curriculum and other activities.
- students understand and follow the Online Safety Policy and acceptable use policies.
- students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices.
- in lessons where internet use is pre-planned students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Online Safety Committee:

The Online Safety Group provides a consultative group that has wide representation from the school community, with responsibility for issues regarding online safety and the monitoring the Online Safety Policy including the impact of initiatives. The group will also be responsible for regular reporting to the Governing Body / Directors.

Members of the Online Safety Group will assist the Online Safety Lead with:

- the production / review / monitoring of the school Online Safety Policy / documents.
- mapping and reviewing the online safety / digital literacy curricular provision – ensuring relevance, breadth and progression.
- monitoring network / internet / incident logs
- consulting stakeholders – including parents / carers and the students about the online safety provision.
- monitoring improvement actions identified through use of the 360-degree safe self-review tool.

Students:

- are responsible for using the school digital technology systems in accordance with the Student Acceptable Use Agreement
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on online bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website / Learning Platform and information about national / local online safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events.
- access to parents' sections of the website / Learning Platform and on-line student records
- their children's personal devices in the school (where this is allowed)

Community Users

Community Users who access school systems / website / Learning Platform as part of the wider school provision will be expected to sign a Community User AUA before being provided with access to school systems.

Policy Statements

Education – Students

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in online safety / digital literacy is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum should be provided as part of Computing / PHSE and other lessons and should be regularly revisited.
- Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities.
- Students should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Students should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- Students should be helped to understand the need for the student Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices.
- in lessons where internet use is pre-planned, it is best practice that students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where students are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g., racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated

person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Education – Parents / Carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of their children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, web site, Learning Platform
- Parents / Carers evenings / sessions
- High profile events / campaigns e.g., Safer Internet Day
- Reference to the relevant web sites / publications e.g. swgfl.org.uk, www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers

Education – The Wider Community

The school will provide opportunities for local community groups and members of the community to gain from the school's online safety knowledge and experience. This may be offered through the following:

- Providing family learning courses in use of new digital technologies, digital literacy and online safety
- Online safety messages targeted towards grandparents and other relatives as well as parents.
- The school website will provide online safety information for the wider community.
- Supporting community groups e.g. Early Years Settings, Childminders, youth / sports / voluntary groups to enhance their Online Safety provision possibly supporting the groups in the use of Online Compass, an online safety self-review tool for groups such as these - www.onlinecompass.org.uk

Education & Training – Staff / Volunteers

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school Online Safety Policy and Acceptable Use Agreements.
- It is expected that some staff will identify online safety as a training need within the performance management process.
- The Online Safety Coordinator will receive regular updates through attendance at external training events (e.g., from SWGfL / LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- This Online Safety Policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The Online Safety Coordinator will provide advice / guidance / training to individuals as required.

Training – Governors

Governors should take part in online safety training and awareness sessions, with particular importance for those who are members of any subcommittee / group involved in technology / online safety / health and safety /safeguarding. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority, National Governors Association or other relevant organisation (e.g., SWGfL).
- Participation in school training / information sessions for staff or parents.

Technical – infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of school technical systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to school technical systems and devices.

- All users will be provided with login credentials by the ICTNS Team, who will keep an up-to-date record of users and their usernames. Users are responsible for the security of their username and password and will be required to change their password every 90 days.
- The "master / administrator" passwords for the school ICT systems, used by the Network Manager must also be available to the Headteacher or other nominated senior leader and kept in a secure place (e.g., school safe).
- The Network Manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated, and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes. Current Smoothwall Amendment Request form can be found here (https://forms.office.com/Pages/ResponsePage.aspx?id=F8ora-u3WkWBk94xFwVnvfHaiNsmHs5PjsuTy1MGDxJUQjQ5WUtBS0xJVTU1QUxRMlpWSVJMMklZNi4u).
- Internet filtering / monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet.
- Smoothwall is set to provide different levels of filtering for staff and students.
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement
- An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person, as agreed. This is covered by the ICTNS support site.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up-to-date endpoint protection software.
- An agreed policy is in place for the provision of temporary access of "guests" (e.g., trainee teachers, supply teachers, visitors) onto the school systems. Our procedure for this, which provides temporary access with no email and limited shared area access, unless it's asked for by the DOL/Line manager.
- An agreed policy is in place regarding the extent of personal use that users (staff / students / community users) and their family members are allowed on school devices that may be used out of school. This is covered by the AUP.

- An agreed policy is in place that all forbids staff from downloading executable files and installing programmes on school devices. This is covered by the AUP.

Mobile Technologies (including BYOD/BYOT)

Mobile technology devices may be school owned or personally owned and might include smartphone, tablet, notebook / laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school's learning platform and other cloud-based services such as email and data storage.

All users should understand that the primary purpose of the use mobile / personal devices in a school context is educational. The mobile technologies policy should be consistent with and inter-related to other relevant school polices including but not limited to the Safeguarding Policy, Behaviour Policy, Bullying Policy, Acceptable Use Policy, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school's Online Safety education programme.

- The school Acceptable Use Agreements for staff, students/students and parents / carers will give consideration to the use of mobile technologies.
- The school allows:

	School Devices			Personal Devices		
	School owned and allocated to a single user	School owned for use by multiple users	Authorised device[1]	Student owned	Staff owned	Visitor owned
Allowed in school	Yes	Yes	Yes	Restricted use only	Yes	Yes
Internet Access only	Yes	Yes	Yes	KS4 Only	Yes	On request (time limited)
Full network access	Yes	Yes*	No	No	No	No

* In so far as the device is capable of accessing school resources.

[1] Authorised device – purchased by the student/family through a school-organised scheme. This device may be given full access to the network as if it were owned by the school

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and students need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing their own images on the internet e.g., on social networking sites.
- Written permission from parents or carers will be obtained before photographs of students are published on the school website / social media / local press.
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other students in the digital / video images.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Any photos taken on personal devices, should be uploaded to the school network (SharePoint) or school run social media, and immediately deleted from the staff member's device.
- Care should be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' / Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Student's / Student's work can only be published with the permission of the student and parents or carers.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.

The school must ensure that:

- It has a Data Protection Policy.
- It has paid the appropriate fee to the Information Commissioner's Office (ICO).
- It has appointed a Data Protection Officer (DPO).
- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Data held must be accurate and up to date. Inaccuracies are corrected without unnecessary delay.
- The lawful basis for processing personal data (including, where relevant, consent) has been identified and documented and details provided in a Privacy Notice. (See Privacy Notice section in the appendix)
- Where special category data is processed, a lawful basis and a separate condition for processing have been identified.
- Data Protection Impact Assessments (DPIA) are carried out before any new services are given access to school data.
- It has clear and understood arrangements for access to and the security, storage and transfer of personal data, including, where necessary, adequate contractual clauses or safeguards where personal data is passed to third parties e.g., cloud service providers.
- Procedures must be in place to deal with the individual rights of the data subject i.e., a Subject Access Requests to see all or a part of their personal data held by the data controller.
- There are clear and understood data retention policies and routines for the deletion and disposal of data.
- There is a policy for reporting, logging, managing and recovering from an information risk incident which recognises the requirement to report relevant data breaches to the ICO within 72 hours of the breach, where feasible.
- Consideration has been given to the protection of personal data when accessed using any remote access solutions.
- All schools have a Freedom of Information Policy which sets out how it will deal with FOI requests.
- All staff receive data handling awareness / data protection training and are made aware of their responsibilities.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, memory stick or any other removable media:

- The data must be encrypted, and password protected. Offsite laptops use Bilocker encryption.
- The device must offer approved virus and malware checking software.
- The data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete. Intune management of iPads and laptops allows devices to be remotely wiped.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

	Staff & other adults				Students			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to the school, remain unseen unless staff allow their use.	✓						✓	
Use of mobile phones in lessons		✓					✓	
Use of mobile phones in social time		✓						✓

Taking photos on mobile phones / cameras	✓						✓	
Use of other mobile devices e.g., tablets, gaming devices			✓				✓	
Use of personal email addresses in school, or on school network	✓					✓		
Use of school email for personal emails				✓				✓
Use of messaging apps	✓							✓
Use of social media	✓							✓
Use of blogs, stories and digital updates	✓						✓	

When using communication technologies, the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are logged.
- Users must immediately report to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and students or parents / carers (email, social media, chat, blogs, VLE etc) must be professional in tone and content.
- Students should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

The school uses interactive storytelling to share with its community events taking place in school throughout the week. This forms an integral aspect to the school's promotional work. The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to students, staff and the school through:

- Ensuring that personal information is not published to the school's "official" Social Media accounts.

- Training is provided including acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions.
- Risk assessment, including legal risk.

School staff should ensure that:

- No direct reference should be made in social media to students, parents / carers or school staff.
- They do not engage in online discussion on personal matters relating to members of the school community.
- Personal opinions should not be attributed to the school.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information. Guidance is provided in the Millais Online site.

When official school social media accounts are established, there should be:

- A process for approval by senior leaders
- Clear processes for the administration and monitoring of these accounts – involving at least two members of staff.
- A code of behaviour for users of the accounts, including
- Systems for reporting and dealing with abuse and misuse.
- Understanding of how incidents may be dealt with under school disciplinary procedures.

Personal Use:

- Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.
- No reference should be made in personal social media accounts to students, parents / carers or school staff.
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy.
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken.
- The school permits reasonable and appropriate access to private social media sites.

Monitoring of Public social media

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school.

The school's use of social media for professional purposes will be checked regularly by the senior risk officer and Online Safety Committee to ensure compliance with the school policies.

Dealing with unsuitable / inappropriate behaviours and activities online (including social media)

Some internet activity e.g., accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities e.g., cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in / or outside the school when using school equipment or systems. The school policy restricts usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	Pornography				X	
	Promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	Promotion of extremism or terrorism				X	
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	

User Actions cont.	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Using school systems to run a private business				X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school				X	
Infringing copyright				X	
Revealing or publicising confidential or proprietary information (e.g., financial / personal information, databases, computer / network access codes and passwords)				X	
Creating or propagating computer viruses or other harmful files				X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)				X	
On-line gaming (educational)		◎			
On-line gaming (non-educational)				X	
On-line gambling				X	
On-line shopping / commerce (staff only)		◎			
File sharing	◎				
Use of social media		◎			
Use of messaging apps			◎		
Use of video broadcasting e.g., YouTube	◎				

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see "User Actions" above).

Please note that all instances of mis-use of social media by students are automatically dealt with using our Anti-Bullying Policy and recommendations due to the imbalance of power assumed by the sharing on a social media platform.

School Actions & Sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:

Students Incidents	Refer to class teacher / tutor	Warning	Refer to DoL and DoY	Inform parents / carers	Refer to Online Safety Lead and Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security etc.	Removal of network / internet access rights	Further sanction e.g., detention / exclusion
Allowing others to access school network by sharing username and passwords		X	X	X	X		X	X	X
Attempting to access or accessing the school network, using another student's / student's account		X	X	X	X		X		X
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X	X	X	X	X	X
Unauthorised use of non-educational sites during lessons	X	X	X	X			X		

Students Incidents cont.	Refer to class teacher / tutor	Warning	Refer to DoL and DoY	Inform parents / carers	Refer to Online Safety Lead and	Refer to Police	Refer to technical support staff for action re filtering / security etc.	Removal of network / internet	Further sanction e.g., suspension
Unauthorised / inappropriate use of mobile phone / digital camera / another mobile device	X	X	X	X	X				X
Unauthorised / inappropriate use of social media / messaging apps / personal email		X	X	X	X				X
Attempting to access or accessing the school network, using the account of a member of staff		X	X	X	X	X	X	X	X
Corrupting or destroying the data of other users	X	X	X	X	X		X	X	X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X	X	X	X	X	X	X
Unauthorised downloading or uploading of files		X	X	X	X		X	X	X
Continued infringements of the above, following previous warnings or sanctions		X		X		X	X	X	X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X	X	X	X	X	X	X	X	X
Using proxy sites or other means to subvert the school's filtering system		X		X	X		X	X	X
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X	X	X	X		X		
Deliberately accessing or trying to access offensive or pornographic material	X	X	X	Inform	X	X	X	X	X

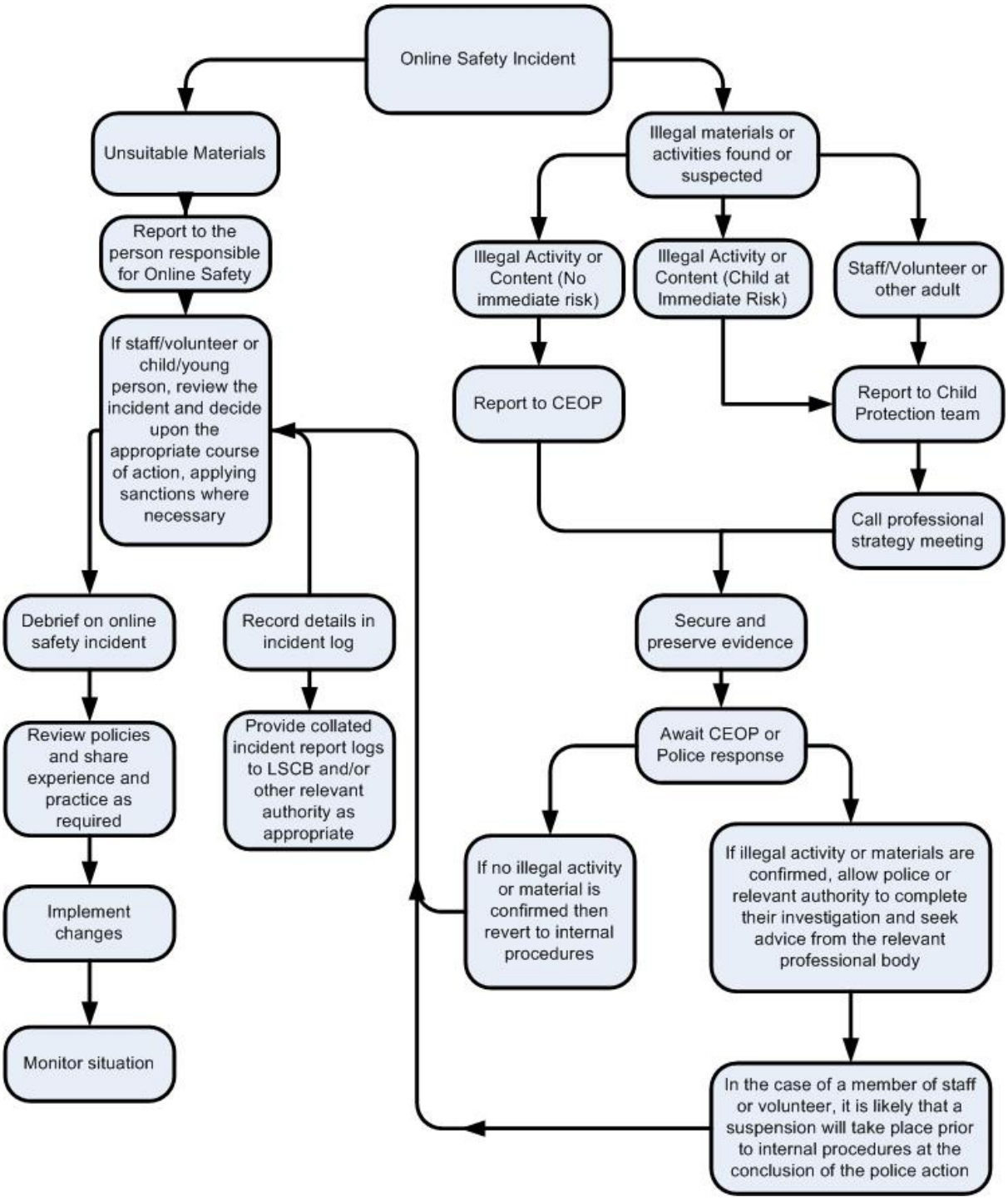
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	X	X	X	X	X	X	X	X	X

Guidance for school staff in dealing with incidents of concern on social media

1. Gather statements as soon as the incident is reported. It's important to include dates of messages, photographic content. Identify if comments have anything of a racist, homophobic, terrorist nature (high level intervention required) or more simply 'general unkindness'.
2. Record on school reporting system for behaviour (Bromcom)
3. If it includes a clip/post, then parents of affected child should report to the social media site and request it is removed due to its nature.
4. The school's investigation of the situation would gather evidence to support the decision of misuse and or cyberbullying. Horsham district council run a mediation service which may assist with this (please see attached).
5. If the comments made on the social media site and potentially on a video involve deformation of character, this is a civil offence. It would depend on what is being said as to whether police would record it as Malicious Communications, but with racial, homophobic or terrorist tones being expressed it is possible.
6. Police can request school statements to check what was witnessed and/or heard if the matter is reported as a racial/hate crime (whether they mention hearing the words or not).
7. Most importantly the school should work on the mediation between the students and offer parents the Horsham District Mediation Service for assistance.

Staff Incidents	Refer to line manager	Refer to Headteacher	Warning	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc.	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	X	X	X	X	X	X	X	X
Inappropriate personal use of the internet / social media / personal email	X	X	X					
Unauthorised downloading or uploading of files	X	X	X			X		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	X	X	X			X		
Careless use of personal data e.g., holding or transferring data in an insecure manner	X	X	X	X		X		
Deliberate actions to breach data protection or network security rules	X	X	X	X		X	X	X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X	X	X	X		X	X	X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X	X	X		X	X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students	X	X	X	X	X	X	X	X
Actions which could compromise the staff member's professional standing	X	X	X	X	X	X	X	X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X	X	X	X	X	X	X	X
Using proxy sites or other means to subvert the school's filtering system	X	X	X	X	X	X	X	X
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X	X	X	X	X		
Deliberately accessing or trying to access offensive or pornographic material	X	X	X	X	X	X	X	X
Breaching copyright or licensing regulations	X	X	X	X	X	X	X	
Continued infringements of the above, following previous warnings or sanctions	X	X	X	X	X	X	X	X

Illegal Incidents



Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary, can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority / Academy Group or national / local organisation (as relevant).
    - Police involvement and/or action
- If content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
    - incidents of 'grooming' behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - promotion of terrorism or extremism
    - other criminal conduct, activity or materials
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

Millais School

Online Safety Policy

Social Media Staff Policy

Social Media Policy

Social media (e.g., Facebook, Twitter, LinkedIn) is a broad term for any kind of online platform which enables people to directly interact with each other. However, some games, for example Minecraft or World of Warcraft and video sharing platforms such as You Tube have social media elements to them.

The school recognises the numerous benefits and opportunities which a social media presence offers. Staff, parents/carers and students/students are actively encouraged to find creative ways to use social media. However, there are some risks associated with social media use, especially around the issues of safeguarding, bullying and personal reputation. This policy aims to encourage the safe use of social media by the school, its staff, parents, carers and children.

As a school we do not officially sanction the use of private Social Media groups of students. Our Online Safety Policy is clear on this. Personal use of apps and Social Media sites are outside of the school's remit, and we cannot be held responsible for the students' activities therein. This does not negate our responsibility to support victims (if the incident causes problems in the school) and educate the students in the safe use of technology.

Scope

This policy is subject to the school's Codes of Conduct and Acceptable Use Agreements.

This policy:

- Applies to all staff and to all online communications which directly or indirectly, represent the school.
- Applies to such online communications posted at any time and from anywhere.
- Encourages the safe and responsible use of social media through training and education.
- Defines the monitoring of public social media activity pertaining to the school.

The school respects privacy and understands that staff and students/students may use social media forums in their private lives. However, personal communications likely to have a negative impact on professional standards and/or the school's reputation are within the scope of this policy.

Professional communications are those made through official channels, posted on a school account or using the school's name. All professional communications are within the scope of this policy.

Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made

clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.

Personal communications which do not refer to or impact upon the school are outside the scope of this policy.

Digital communications with students/students are also considered. Staff may use social media to communicate with learners via a school social media account for teaching and learning purposes but must consider whether this is appropriate and consider the potential implications.

Organisational control

Roles & Responsibilities

- SLT
    - Facilitating training and guidance on Social Media use.
    - Developing and implementing the Social Media policy
    - Taking a lead role in investigating any reported incidents.
    - Making an initial assessment when an incident is reported and involving appropriate staff and external agencies as required.
    - Receive completed applications for social media accounts
    - Approve account creation.
- Administrator / Moderator
    - Create the account following SLT approval.
    - Store account details, including passwords securely.
    - Be involved in monitoring and contributing to the account.
    - Control the process for managing an account after the lead staff member has left the organisation (closing or transferring)
- Staff
    - Know the contents of and ensure that any use of social media is carried out in line with this and other relevant policies.
    - Attending appropriate training
    - Regularly monitoring, updating and managing content he/she has posted via school accounts.
    - Adding an appropriate disclaimer to personal accounts when naming the school

Existing & New accounts

The school works closely with Interactive our website host. They provide us with interactive social media accounts that work with the website to tell our story. @ and # are used to pull stories together and share with a wider audience. Staff training takes place to ensure staff feel able to share their departmental stories in the correct way. An example of this training is here : How to tell your story using an Iphone .docx

Monitoring

School accounts must be monitored regularly and frequently (preferably 7 days a week, including during holidays). W**e generally turn off comments when posting to avoid any negative comments**.

Behaviour

- The school requires that all users using social media adhere to the standard of behaviour as set out in this policy and other relevant policies.
- Digital communications by staff must be professional and respectful at all times and in accordance with this policy. Staff will not use social media to infringe on the rights and privacy of others or make ill-considered comments or judgments about staff. School social media accounts must not be used for personal gain. Staff must ensure that confidentiality is maintained on social media even after they leave the employment of the school.
- Users must declare who they are in social media posts or accounts. Anonymous posts are discouraged in relation to school activity.
- If a journalist makes, contact about posts made using social media staff must follow the school media policy before responding.
- Unacceptable conduct, (e.g., defamatory, discriminatory, offensive, harassing content or a breach of data protection, confidentiality, copyright) will be considered extremely seriously by the school and will be reported as soon as possible to a relevant senior member of staff, and escalated where appropriate.
- The use of social media by staff while at work may be monitored, in line with school policies. The school permits reasonable and appropriate access to private social media sites. However, where excessive use is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken.
- The school will take appropriate action in the event of breaches of the social media policy. Where conduct is found to be unacceptable, the school will deal with the matter internally. Where conduct is considered illegal, the school will report the matter to the police and other relevant external agencies and may take action according to the disciplinary policy.

Legal considerations

- Users of social media should consider the copyright of the content they are sharing and, where necessary, should seek permission from the copyright holder before sharing.
- Users must ensure that their use of social media does not infringe upon relevant data protection laws, or breach confidentiality.

Handling abuse

- When acting on behalf of the school, handle offensive comments swiftly and with sensitivity.
- If a conversation turns and becomes offensive or unacceptable, school users should block, report or delete other users or their comments/posts and should inform the audience exactly why the action was taken.
- If you feel that you or someone else is subject to abuse by colleagues through use of a social networking site, then this action must be reported using the agreed school protocols.

Tone

The tone of content published on social media should be appropriate to the audience, whilst retaining appropriate levels of professional standards. Key words to consider when composing messages are:

- Engaging
- Conversational
- Informative
- Friendly (on certain platforms, e.g., Facebook)

Use of images

School use of images can be assumed to be acceptable, providing the following guidelines are strictly adhered to.

- Permission to use any photos or video recordings should be sought in line with the school's digital and video images policy. If anyone, for any reason, asks not to be filmed or photographed then their wishes should be respected.
- Under no circumstances should staff share or upload student pictures online other than via school owned social media accounts
- Staff should exercise their professional judgement about whether an image is appropriate to share on school social media accounts. Students should be appropriately dressed, not be subject to ridicule and must not be on any school list of children whose images must not be published.
- If a member of staff inadvertently takes a compromising picture which could be misconstrued or misused, they must delete it immediately.

Personal use

- Staff
    - Personal communications are those made via a personal social media account. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.
    - Personal communications which do not refer to or impact upon the school are outside the scope of this policy.
    - Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken.
    - The school permits reasonable and appropriate access to private social media sites.
- Students
    - Staff are not permitted to follow or engage with current or prior students of the school on any personal social media network account. Staff who have family as current or former students are exempt from this.
    - The school's education programme should enable the students/students to be safe and responsible users of social media.
    - Students/students are encouraged to comment or post appropriately about the school. Any offensive or inappropriate comments will be resolved by the use of the school's behaviour policy.
- Parents/Carers
    - If parents/carers have access to a school learning platform where posting or commenting is enabled, parents/carers will be informed about acceptable use.
    - The school has an active parent/carer education programme which supports the safe and positive use of social media. This includes information on the website.
    - 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, refer parents to the school's complaints procedures.

Monitoring posts about the school

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school.
- The school should effectively respond to social media comments made by others according to a defined policy or process.

Appendix

Managing your personal use of social media:

- "Nothing" on social media is truly private.
- Social media can blur the lines between your professional and private life. Don't use the school logo and/or branding on personal accounts.
- Check your settings regularly and test your privacy.
- Keep an eye on your digital footprint.
- Keep your personal information private.
- Regularly review your connections – keep them to those you want to be connected to
- When posting online consider; Scale, Audience and Permanency of what you post.
- If you want to criticise, do it politely.
- Take control of your images – do you want to be tagged in an image? What would children or parents say about you if they could see your images?
- Know how to report a problem.

Managing school social media accounts

The Do's

- Check with a senior leader before publishing content that may have controversial implications for the school.
- Use a disclaimer when expressing personal views.
- Make it clear who is posting content.
- Use an appropriate and professional tone.
- Be respectful to all parties.
- Ensure you have permission to 'share' other peoples' materials and acknowledge the author.
- Express opinions but do so in a balanced and measured manner
- Think before responding to comments and, when in doubt, get a second opinion.
- Seek advice and report any mistakes using the school's reporting process.
- Consider turning off tagging people in images where possible.

The Don'ts

- Don't make comments, post content or link to materials that will bring the school into disrepute.
- Don't publish confidential or commercially sensitive material.
- Don't breach copyright, data protection or other relevant legislation.
- Consider the appropriateness of content for any audience of school accounts, and don't link to, embed or add potentially inappropriate content.
- Don't post derogatory, defamatory, offensive, harassing or discriminatory content.
- Don't use social media to air internal grievances.

Millais School

Online Safety Policy

School Policy : Electronic Devices – Searching and Deletion

School Policy: Electronic Devices - Searching & Deletion

Introduction

The changing face of information technologies and ever-increasing student use of these technologies has meant that the Education Acts have had to change in an attempt to keep pace. Within Part 2 of the Education Act 2011 (Discipline) there have been changes to the powers afforded to schools by statute to search students in order to maintain discipline and ensure safety. Schools are required to ensure they have updated policies which take these changes into account. No such policy can, on its own, guarantee that the school will not face legal challenge, but having a robust policy which takes account of the Act, and applying it in practice, will however help to provide the school with justification for what it does.

The particular changes we deal with here are the added power to search for items 'banned under the school rules' and the power to 'delete data' stored on seized electronic devices.

Items banned under the school rules are determined and publicised by the Headteacher (section 89 Education and Inspections Act 1996).

An item banned by the school rules may only be searched for under these new powers if it has been identified in the school rules as an item that can be searched for. It is therefore important that there is a school policy which sets out clearly and unambiguously the items which:

- are banned under the school rules; and
- are banned AND can be searched for by authorised school staff.

The act allows authorised persons to examine data on electronic devices if they think there is a good reason to do so. In determining a 'good reason' to examine or erase the data or files the authorised staff member must reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or could break the school rules.

Following an examination, if the person has decided to return the device to the owner, or to retain or dispose of it, they may erase any data or files, if they think there is a good reason to do so.

The Head Teacher must publicise the school behaviour policy, in writing, to staff, parents / carers and students at least once a year. There are clear links between the search and deletion policy and the behaviour policy.

Relevant legislation:

- Education Act 1996
- Education and Inspections Act 2006

- Education Act 2011 Part 2 (Discipline)
- The School Behaviour (Determination and Publicising of Measures in Academies) Regulations 2012
- Health and Safety at Work etc. Act 1974
- Obscene Publications Act 1959
- Children Act 1989
- Human Rights Act 1998
- Computer Misuse Act 1990

This is not a full list of Acts involved in the formation of this advice. Further information about relevant legislation can be found via the above link to the DfE advice document.

Responsibilities

This policy has been written by and will be reviewed by: Chantal Warwick : Assistant Headteacher

The Headteacher has authorised the following members of staff to carry out searches for and of electronic devices and the deletion of data / files on those devices : Deputy Headteacher, M. Sutton and Assistant Headteacher, C. Warwick

Training / Awareness

Members of staff should be made aware of the school's policy on "Electronic devices – searching and deletion":

- at induction
- at regular updating sessions on the school's online safety policy

Members of staff authorised by the Headteacher to carry out searches for and of electronic devices and to access and delete data / files from those devices should receive training that is specific and relevant to this role.

Specific training is required for those staff who may need to judge whether material that is accessed is inappropriate or illegal.

Policy Statements

Search:

The school Behaviour Policy refers to the policy regarding searches with and without consent for the wide range of items covered within the Education Act 2011 and lists those items. This policy refers only to the searching for and of electronic devices and the deletion of data / files on those devices.

Students are allowed to bring mobile phones or other personal electronic devices to school and use them only within the rules laid down by the school.

Any misuse of a mobile device should be reported and logged appropriately with the Headteacher's PA. The sanctions for this breach are First offence – confiscation – student collect at end of day; Second offence – confiscation – parent requested to pick up; Third offence – confiscation – parent asked to pick up and further sanction agreed with parent.

Where a student has used their phone in a manner that breaches the school's safeguarding policy then these steps may be escalated and either a) material on the phone deleted or b) the phone seized to support further investigation, potentially with the police involved. The school reserves the right to conduct bag searches to retrieve items that may pose harm or safeguarding concerns to students.

Authorised staff (defined in the responsibilities section above) have the right to search for such electronic devices where they reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the school rules.

- Searching with consent - Authorised staff may search with the student's consent for any item
- Searching without consent - Authorised staff may only search without the student's consent for anything which is either 'prohibited' (as defined in Section 550AA of the Education Act 1996) or appears in the school rules as an item which is banned and may be searched for

In carrying out the search:

The authorised member of staff must have reasonable grounds for suspecting that a student is in possession of a prohibited item i.e., an item banned by the school rules and which can be searched for.

The authorised member of staff should take reasonable steps to check the ownership of the mobile phone / personal electronic device before carrying out a search. The powers included in the Education Act do not extend to devices owned (or mislaid) by other parties e.g., a visiting parent or contractor, only to devices in the possession of students / students.

The authorised member of staff should take care that, where possible, searches should not take place in public places e.g., an occupied classroom, which might be considered as exploiting the student being searched.

The authorised member of staff carrying out the search must be the same gender as the student being searched; and there must be a witness (also a staff member) and, if at all possible, they too should be the same gender as the student/ student being searched.

There is a limited exception to this rule: Authorised staff can carry out a search of a student of the opposite gender including without a witness present, but only where you reasonably believe that there is a risk that serious harm will be caused to a person if you do not conduct the search immediately and where it is not reasonably practicable to summon another member of staff.

Extent of the search:

The person conducting the search may not require the student to remove any clothing other than outer clothing.

Outer clothing means clothing that is not worn next to the skin or immediately over a garment that is being worn as underwear (outer clothing includes hats; shoes; boots; coat; blazer; jacket; gloves and scarves).

'Possessions' means any goods over which the student has or appears to have control – this includes desks, lockers and bags.

A student's possessions can only be searched in the presence of the student and another member of staff, except where there is a risk that serious harm will be caused to a person if the search is not conducted immediately and where it is not reasonably practicable to summon another member of staff.

The power to search without consent enables a personal search, involving removal of outer clothing and searching of pockets; but not an intimate search going further than that, which only a person with more extensive powers (e.g., a police officer) can do.

Use of Force – force cannot be used to search without consent for items banned under the school rules regardless of whether the rules say an item can be searched for.

Electronic devices:

An authorised member of staff finding an electronic device may access and examine any data or files on the device if they think there is a good reason to do so (i.e., the staff member must reasonably suspect

that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the school rules).

The examination of the data / files on the device should go only as far as is reasonably necessary to establish the facts of the incident. Any further intrusive examination of personal data may leave the school open to legal challenge.

If inappropriate material is found on the device it is up to the authorised member of staff to decide whether they should delete that material, retain it as evidence (of a criminal offence or a breach of school discipline) or whether the material is of such seriousness that it requires the involvement of the police. Examples of illegal activity would include:

- child sexual abuse images (including images of one child held by another child)
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

Deletion of Data

Following an examination of an electronic device, if the authorised member of staff has decided to return the device to the owner, or to retain or dispose of it, they may erase any data or files, if they think there is a good reason to do so.

If inappropriate material is found on the device, it is up to the authorised member of staff to decide whether they should delete that material, retain it as evidence (of a possible criminal offence or a breach of school discipline) or whether the material is of such seriousness that it requires the involvement of the police.

A record should be kept of the reasons for the deletion of data / files. Records will also help the school to review online safety incidents, learn from what has happened and adapt and report on application of policies as necessary.

Care of Confiscated Devices

School staff are reminded of the need to ensure the safe keeping of confiscated devices, to avoid the risk of compensation claims for damage / loss of such.

Audit / Monitoring / Reporting / Review

The responsible person, the Deputy Headteacher, will ensure that full records are kept of incidents involving the searching for and of mobile phones and electronic devices and the deletion of data / files.

These records will be reviewed by the Online Safety Committee and Online Safety Governor at regular intervals

This policy will be reviewed by the head teacher and governors annually and in response to changes in guidance and evidence gained from the records.

Millais School

Online Safety Policy

Mobile Technologies Policy

Mobile Technologies Policy (inc. BYOD/BYOT)

Mobile technology devices may be a school owned or privately-owned smartphone, tablet, notebook / laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school's learning platform and other cloud-based services such as email and data storage.

The absolute key consideration in the use of mobile technologies is that the students, staff and wider school community understand that the primary purpose of having their personal device at school is educational and that this is irrespective of whether the device is school owned or personally owned. This mobile technologies policy sits alongside a range of polices including but not limited to the Safeguarding Policy, Bullying Policy, Acceptable Use Policy, policies around theft or malicious damage and the Behaviour Policy. Teaching about the safe and appropriate use of mobile technologies should be included in the online safety education programme.

The school has provided technical solutions for the safe use of mobile technology for school devices/personal devices :

- All school devices are controlled though the use of Mobile Device Management software
- Appropriate access control is applied to all mobile devices according to the requirements of the user (e.g., Internet only access, network access allowed, shared folder network access)
- For all mobile technologies, filtering will be applied to the internet connection and attempts to bypass this are not permitted
- Appropriate exit processes are implemented for devices no longer used at a school location or by an authorised user.
- All school devices are subject to routine monitoring
- Pro-active monitoring has been implemented to monitor activity

When personal devices are permitted:

- Personal devices are brought into the school entirely at the risk of the owner and the decision to bring the device in to the school lies with the user (and their parents/carers) as does the liability for any loss or damage resulting from the use of the device in school
- The school accepts no responsibility or liability in respect of lost, stolen or damaged devices while at school or on activities organised or undertaken by the school (the school recommends insurance is purchased to cover that device whilst out of the home)

- The school accepts no responsibility for any malfunction of a device due to changes made to the device while on the school network or whilst resolving any connectivity issues
- The school recommends that the devices are made easily identifiable and have a protective case to help secure them as the devices are moved around the school. Passcodes or PINs should be set on personal devices to aid security
- The school is not responsible for the day-to-day maintenance or upkeep of the user's personal device such as the charging of any device, the installation of software updates or the resolution of hardware issues

Users are expected to act responsibly, safely and respectfully in line with current Acceptable Use Agreements, in addition.

- Devices may not be used in tests or exams
- Visitors should be provided with information about how and when they are permitted to use mobile technology in line with local safeguarding arrangements
- Users are responsible for keeping their device up to date through software, security and app updates. The device is virus protected and should not be capable of passing on infections to the network
- Users are responsible for charging their own devices and for protecting and looking after their devices while in school
- Personal devices should be charged before being brought to school as the charging of personal devices is not permitted during the school day
- Devices must be in silent mode on the school site and on school buses
- School devices are provided to support learning. It is expected that students will bring devices to school as required.
- Confiscation and searching (England) - the school has the right to take, examine and search any device that is suspected of unauthorised use, either technical or inappropriate.
- The school will ensure that school devices contain the necessary apps for schoolwork. Apps added by the school will remain the property of the school and will not be accessible to students on authorised devices once they leave the school roll. Any apps bought by the user on their own account will remain theirs.
- Users should be mindful of the age limits for app purchases and use and should ensure they read the terms and conditions before use.
- Users must only photograph people with their permission. Users must only take pictures or videos that are required for a task or activity. All unnecessary images or videos will be deleted immediately
- Devices may be used in lessons in accordance with teacher direction

- Staff owned devices should not be used for personal purposes during teaching sessions, unless in exceptional circumstances
- Printing from personal devices will not be possible

Millais School

Online Safety Policy

School Technical Security Policy

(Including filtering and passwords)

Introduction

Effective technical security depends not only on technical measures, but also on appropriate policies and procedures and on good user education and training. The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that:

- users can only access data to which they have right of access
- no user should be able to access another's files (other than that allowed for monitoring purposes within the school's policies). Exemption is made for ICTNS staff when required by their duties.
- access to personal data is securely controlled in line with the school's personal data policy
- logs are maintained of access by users and of their actions while users of the system
- there is effective guidance and training for users
- there are regular reviews and audits of the safety and security of school computer systems
- there is oversight from senior leaders, and these have impact on policy and practice.

Responsibilities

The management of technical security will be the responsibility of the Network Manager and team of Technical Staff.

Technical Security

Policy statements

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented.

It will also need to ensure that the relevant people receive guidance and training and will be effective in carrying out their responsibilities

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- Appropriate security measures are in place to protect the servers, firewalls, switches, routers, wireless systems, workstations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data.
- Responsibilities for the management of technical security are clearly assigned to appropriate and well-trained staff.
- All users will have clearly defined access rights to school technical systems. Details of the access rights available to groups of users will be recorded by the Network Manager / Technical Staff (or other person) and will be reviewed, at least annually, by the Online Safety Group.
- Users will be made responsible for the security of their username and password must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- ICTNS Manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- Mobile device security and management procedures are in place
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- Remote management tools are used by staff to control workstations and view user's activity
- An appropriate system is in place for users to report any actual / potential technical incident to the Network Manager.
- An agreed policy is in place for the provision of temporary access of "guests" (e.g., trainee teachers, supply teachers, visitors) onto the school system. *Millais has three tiers of temporary access. Non-teaching visitors or guest speakers are only given network/internet access upon request. If only internet access is required, a login for the Millais Visitors wireless is provided, this allows access to the internet but no the Millais network. If required, network access is provided using single use accounts assigned to individual. These accounts are only given access to the "public" data and applications. Short term supply teachers are given network accounts with read-only access to the Shared Area and teaching resources. This is provided through reusable accounts assigned to the individual, they have access to the school's general applications including Bromcom. Long term supply or trainee teachers will be asked to sign the staff AUP. Once this is done, they will be given the same on-site access as contracted teaching staff.*

- An agreed policy is in place regarding the downloading of executable files and the installation of programmes on school devices by users. *As described in the Staff and Visitor AUP, users should not download or attempt to run executable files. If a program is required, details of the program (along with any download links) should be submitted to ICTNS via the Director of Learning. Depending on the program, this may have to be signed off by the safeguarding lead and/or Data Protection Officer. If the program requires access to staff or student data (for example for account creation) a GDPR audit will need to be carried out and the results kept on file by the DPO.*
- An agreed policy is in place regarding the extent of personal use that users (staff / students / community users) and their family members are allowed on school devices that may be used out of school. *Staff are allowed reasonable use of school owned devices for personal use outside of their normal working hours. Staff must ensure their use of school software or services does not breach the licencing conditions of this software (any such breach could result in access to this software / service being suspended). School devices linked to a user's network account (e.g., iPads or staff home-use laptops) should not be used by family members as this presents a substantial risk of data breach. Should family members require access to school devices they should be set up with visitor accounts as described above.*
- An agreed policy is in place regarding the use of removable media (e.g., memory sticks / CDs / DVDs) by users on school devices. *All data storage should be regularly checked to be virus free (this will happen automatically when used on school computers). If data is saved to removeable media that media should be encrypted/password protected. Staff should be aware that anything saved to removeable media will not be backed up by the school, and if lost or damaged will not be recoverable.*
- The school infrastructure and individual workstations are protected by up-to-date software to protect against malicious threats from viruses, worms, trojans etc
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured. *Data should only be removed from the network via encrypted transmission/storage media (as described in the Staff & Visitor AUP). Large quantities of data or sensitive data should only be removed from the school network with the permission of the Head Teacher. The school provides the tools necessary for the safe transmission of data through Office 365 or password protected USB drives.*

Password Security

A safe and secure user authentication system is essential if the above is to be established and will apply to all school technical systems, including networks, devices, email and Virtual Learning Environment (VLE).

Policy Statements

- All users will have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the Network Manager (or other person) and will be reviewed, at least annually, by the Online Safety Group.
- All school networks and systems will be protected by secure passwords that are regularly changed
- The "master / administrator" passwords for the school systems, used by the technical staff, must also be available to the Headteacher or other nominated senior leader and kept in a secure place e.g., school safe.
- All users (adults and young people) will have responsibility for the security of their username and password must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- Passwords for new users, and replacement passwords for existing users will be allocated by the ICTNS Team and (in the case of replacement passwords) the ICT teachers and librarians. Any changes carried out must be notified to the manager of the password security policy (above).
- Users will change their passwords at regular intervals – as described in the staff and student sections
- Where passwords are set / changed manually requests for password changes should be authenticated by the Network Manager to ensure that the new password can only be passed to the genuine individual.

Staff Passwords

- All staff users will be provided with login credentials by the ICTNS Team who will keep an up-to-date record of users and their usernames.
- the password should be a minimum of 8 characters long and must include three of – uppercase character, lowercase character, number, special characters
- must not include proper names or any other personal information about the user that might be known by others
- the account will be "locked out" following ten successive incorrect log-on attempts within thirty minutes.
- temporary passwords e.g., used with new user accounts or when users have forgotten their passwords, shall be enforced to change immediately upon the next account log-on
- passwords shall not be displayed on screen, and shall be securely hashed (use of one-way encryption)
- passwords should be different for different accounts, to ensure that other systems are not put at risk if one is compromised and should be different for systems used inside and outside of school
- should be changed at least every 90 days

- should not re-use for 6 months and be significantly different from previous passwords created by the same user. The last ten passwords cannot be re-used.

Student Passwords

- All users will be provided with a username and password by the ICTNS Team who will keep an up-to-date record of users and their usernames.
- Users will be required to change their password every 365 days
- Students will be taught the importance of password security

Training / Awareness

Members of staff will be made aware of the school's password policy:

- at induction
- through the school's online safety policy and password security policy
- through the Acceptable Use Agreement

Students will be made aware of the school's password policy:

- in lessons: New students are asked to change their password during their first IT/Computing lesson, at which point the school's password policy is described.
- when using the school facilities change their password (in the LRC or with ICT Support) this policy is reinforced.
- through the Acceptable Use Agreement

Audit / Monitoring / Reporting / Review

The ICTNS Team will ensure that full records are kept of:

- User Ids and requests for password changes
- User logins
- Security incidents related to this policy

Filtering

Introduction

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so, because the content on the web changes dynamically and new technologies are constantly being developed. It is important, therefore, to understand that filtering is only

one element in a larger strategy for online safety and acceptable use. It is important that the school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.

Responsibilities

The responsibility for the management of the school's filtering policy will be held by the Network Manager They will manage the school filtering, in line with this policy and will keep records / logs of changes and of breaches of the filtering systems.

To ensure that there is a system of checks and balances and to protect those responsible, changes to the school filtering service must

- be logged in change control logs
- be reported to a second responsible person – The DSL
- either… be reported to and authorised by a second responsible person prior to changes being made.
- be reported to the Online Safety Group every 12 weeks in the form of an audit of the change control logs

All users have a responsibility to report immediately to the Network Manager or DSL any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.

Users must not attempt to use any programmes or software that might allow them to bypass the filtering / security systems in place to prevent access to such materials.

Policy Statements

Internet access is filtered for all users. Differentiated internet access is available for staff and customised filtering changes are managed by the school. Illegal content is filtered by the filtering provider by actively employing the Internet Watch Foundation CAIC list and other illegal content lists. Filter content lists are regularly updated, and internet use is logged and frequently monitored. The monitoring process alerts the school to breaches of the filtering policy, which are then acted upon. There is a clear route for reporting and managing changes to the filtering system. Where personal mobile devices are allowed internet access through the school network, filtering will be applied that is consistent with school practice.

- The school manages its own filtering service

- The school has provided enhanced / differentiated user-level filtering using the Smoothwall filtering platform. (allowing different filtering levels for different year groups and different groups of users – staff / students / students etc.)
- In the event of the technical staff needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher (or other nominated senior leader).
- Mobile devices that access the school internet connection (whether school or personal devices) will be subject to the same filtering standards as other devices on the school systems
- Any filtering issues should be reported immediately to the filtering provider.
- Requests from staff for sites to be removed from the filtered list will be considered by the ICTNS staff. If the request is agreed, this action will be recorded, and logs of such actions shall be reviewed regularly by the Online Safety Group.

Education / Training / Awareness

Students will be made aware of the importance of filtering systems through the online safety education programme. They will also be warned of the consequences of attempting to subvert the filtering system.

Staff users will be made aware of the filtering systems through:

- the Acceptable Use Agreement
- induction training
- staff meetings, briefings, Inset.

Parents will be informed of the school's filtering policy through the Acceptable Use Agreement and through online safety awareness sessions and the Millais Online site.

Changes to the Filtering System

In this section the school should provide a detailed explanation of:

- Staff users may submit a "Smoothwall Amendment Request Form", this should be countersigned by the staff member's Director of Learning or Line Manager. The request is then checked and approved by the DSL or Head Teacher and passed on to the ICTNS Team to be actioned.
- A site will be unblocked if the request meets the following criteria:
    - There is a defined educational requirement for the site and no alternatives are available.
    - The Site is deemed safe and appropriate by the DSL.
    - The proposed use of the site would not be in breach of the school's AUP.

    - It is technically possible to unblock the site and its contents safely (for example, a site servicing YouTube videos could not be fully unblocked for students as this would require unblocking YouTube for students).
- All web filtering requests should be signed off by the DSL and the direct DOL or line manager of the requester.
- "Smoothwall Amendment Request Form" will be kept by ICTNS as a proof the request was actioned.

Users who gain access to, or have knowledge of others being able to access, sites which they feel should be filtered (or unfiltered) should report this in the first instance to the DSL will decide whether to make school level changes (as above).

Monitoring

No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network and on school equipment as indicated in the School Online Safety Policy and the Acceptable Use Agreement. Monitoring will take place as follows:

Millais School uses Smoothwall Monitor (formerly Visigo) monitoring system. This system uses key-stroke monitoring checked against a pre-defined list of safeguarding trigger words/phrases.

Audit / Reporting

Logs of filtering change controls and of filtering incidents will be made available to:

- The Senior Leadership Team.
- Online Safety Group
- Online Safety Governor / Governors committee
- External Filtering provider / Local Authority / Police on request

The filtering policy will be reviewed in the response to the evidence provided by the audit logs of the suitability of the current provision.

Further Guidance

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" (Revised Prevent Duty Guidance: for England and Wales, 2015).

Furthermore the Department for Education published proposed changes to 'Keeping Children Safe in Education' for consultation in December 2015. Amongst the proposed changes, schools will be obligated to "ensure appropriate filters and appropriate monitoring systems are in place. Children should not be able to access harmful or inappropriate material from the school or colleges 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."

In response UKSIC produced guidance on – information on "Appropriate Filtering"

NEN Technical guidance: http://www.nen.gov.uk/e-security-managing-and-maintaining-e-securitycyber-security-in-schools/

Somerset Guidance for schools – this checklist is particularly useful where a school uses external providers for its technical support / security: https://360safe.org.uk/Files/Documents/Somerset-Questions-for-Technical-Support-v4.aspx

Millais School

Online Safety Policy

– Online Safety Committee Terms of Reference

School Policy – Online Safety Committee Terms of Reference

1. Purpose

To provide a consultative group that has wide representation from the school community, with responsibility for issues regarding online safety and the monitoring the online safety policy including the impact of initiatives.

2. Membership

2.1. The online safety group will seek to include representation from all stakeholders.

The composition of the group should include:

- SLT member/s
- Child Protection/Safeguarding officer
- Teaching staff member
- Support staff member
- Online safety coordinator (not ICT coordinator by default)
- Governor
- Parent / Carer
- ICT Technical Support staff (where possible)
- Community users (where appropriate)
- Student representation – for advice and feedback. Student voice is essential in the make-up of the online safety group, but students would only be expected to take part in committee meetings were deemed relevant.

2.2. Other people may be invited to attend the meetings at the request of the Chairperson on behalf of the committee to provide advice and assistance where necessary.

2.3. Committee members must declare a conflict of interest if any incidents being discussed directly involve themselves or members of their families.

2.4. Committee members must be aware that many issues discussed by this group could be of a sensitive or confidential nature.

2.5. When individual members feel uncomfortable about what is being discussed they should be allowed to leave the meeting with steps being made by the other members to allow for these sensitivities

3. Chairperson

The Committee should select a suitable Chairperson from within the group. Their responsibilities include:

- Scheduling meetings and notifying committee members.

- Inviting other people to attend meetings when required by the committee.
- Guiding the meeting according to the agenda and time available.
- Ensuring all discussion items end with a decision, action or definite outcome.
- Making sure that notes are taken at the meetings and that these with any action points are distributed as necessary.

4. Duration of Meetings

Meetings shall be held biannually in July (for the year ahead) and February for review, for a period of one hour. A special or extraordinary meeting may be called when and if deemed necessary.

5. Functions

These are to assist the Online Safety Lead (or another relevant person) with the following

- To keep up to date with new developments in the area of online safety
- To (at least) annually review and develop the online safety policy in line with new technologies and incidents.
- To monitor the delivery and impact of the online safety policy
- To monitor the log of reported online safety incidents (anonymous) to inform future areas of teaching / learning / training.
- To co-ordinate consultation with the whole school community to ensure stakeholders are up to date with information, training and/or developments in the area of online safety. This is carried out through:
- Staff meetings
- Student forums (for advice and feedback)
- Governors meetings
- Surveys/questionnaires for students, parents / carers and staff
- Parents evenings
- Website/VLE/Newsletters
- Online safety events
- Internet Safety Day (annually held on the second Tuesday in February)
- To ensure that monitoring is carried out of Internet sites used across the school.
- To monitor filtering / change control logs (e.g., requests for blocking / unblocking sites).
- To monitor the safe use of data across the school
- To monitor incidents involving cyberbullying for staff and students

6. Amendments

The terms of reference shall be reviewed annually from the date of approval. They may be altered to meet the current needs of all committee members, by agreement of the majority.

The above Terms of Reference for Millais School have been agreed.

Signed by (SLT): ..... Date: .....

Date for review: .....

Millais School

Online Safety Policy

Legislation

Legislation

It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

It is recommended that legal advice is sought in the advent of an e safety issue or situation.

Computer Misuse Act 1990

This Act makes it an offence to:

- Erase or amend data or programs without authority.
- Obtain unauthorised access to a computer.
- "Eavesdrop" on a computer.
- Make unauthorised use of computer time or facilities.
- Maliciously corrupt or erase data or programs.
- Deny access to authorised users.

Data Protection Act 1998

This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept longer than necessary.
- Processed in accordance with the data subject's rights.
- Secure.
- Not transferred to other countries without adequate protection.

Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications Act 2003

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent there is no need to prove any intent or purpose.

Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or another article to another person.

Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts.
- Ascertain compliance with regulatory or self-regulatory practices or procedures.
- Demonstrate standards, which are or ought to be achieved by persons using the system.
- Investigate or detect unauthorised use of the communications system.
- Prevent or detect crime or in the interests of national security.
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
- Ascertain whether the communication is business or personal.
- Protect or support help line staff.
- The school reserves the right to monitor its systems and communications in line with its rights under this act.

Trademarks Act 1994

This provides protection for Registered Trademarks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trademarks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work

has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g., YouTube).

Telecommunications Act 1984

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Protection of Children Act 1978

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is a anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison

Sexual Offences Act 2003

A grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence. Children, Families and Education Directorate page 38 April 2007.

Obscene Publications Act 1959 and 1964

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Human Rights Act 1998

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of "higher law", affecting all other laws. In the school context, human rights to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

The Education and Inspections Act 2006

Empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

The Education and Inspections Act 2011

Extended the powers included in the 2006 Act and gave permission for Headteachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data. http://www.education.gov.uk/schools/studentsupport/behaviour/behaviourpolicies/f0076897/screening-searching-and-confiscation)

The Protection of Freedoms Act 2012

Requires schools to seek permission from a parent / carer to use Biometric systems

The School Information Regulations 2012

Requires schools to publish certain information on its website:

https://www.gov.uk/guidance/what-maintained-schools-must-publish-online

Serious Crime Act 2015

Introduced new offence of sexual communication with a child. Also created new offences and orders around gang crime (including CSE)

Millais School

Online Safety Policy

Guidance used in the writing of this policy

School Personal Data Advice and Guidance

This document is for advice and guidance purposes only. This document is not intended to provide legal advice and the school is encouraged to seek their own legal counsel when considering their management of personal data.

School Personal Data Handling

Recent publicity about data breaches suffered by organisations and individuals continues to make the area of personal data protection a current and high-profile issue for schools, academies and other organisations. It is important that the school has a clear and well understood personal data handling policy in order to minimise the risk of personal data breaches. A breach may arise from a theft, a deliberate attack on your systems, the unauthorised or malicious use of personal data by a member of staff, accidental loss, or equipment failure. In addition:

- No school or individual would want to be the cause of a data breach, particularly as the impact of data loss on individuals can be severe and cause extreme embarrassment, put individuals at risk and affect personal, professional or organisational reputation.
- Schools are "data rich" and the introduction of electronic storage and transmission of data has created additional potential for the loss of data
- The school will want to avoid the criticism and negative publicity that could be generated by any personal data breach.
- The school is subject to a wide range of legislation related to data protection and data use, with significant penalties for failure to observe the relevant legislation.
- It is a legal requirement for all schools to have a Data Protection Policy.

Schools have always held personal data on the students in their care, and increasingly this data is held digitally and accessible not just in the school but also from remote locations. It is important to stress that the data protection laws apply to all forms of personal data, regardless of whether it is held on paper or in electronic format. However, as it is part of an overall online safety policy template, this document will place particular emphasis on data which is held or transferred digitally.

Schools will need to carefully review their policy, in the light of pertinent Local Authority / Parent Organisation regulations and guidance and changes in legislation.

Introduction

Schools and their employees must do everything within their power to ensure the safety and security of any material of a personal or sensitive nature, including personal data.

It is the responsibility of all members of the school community to take care when handling, using or transferring personal data that it cannot be accessed by anyone who does not:

- have permission to access that data
- need to have access to that data.

Data breaches can have serious effects on individuals and / or institutions concerned, can bring the school into disrepute and may well result in disciplinary action, criminal prosecution and fines imposed by the Information Commissioner's Office. Particularly, all transfer of data is subject to risk of loss or contamination.

Anyone who has access to personal data must know, understand and adhere to the relevant school policy which brings together the statutory requirements contained in relevant data protection legislation and relevant regulations and guidance (where relevant from the Local Authority / Parent Organisation).

Legislative Context

With effect from 25th May 2018, the data protection arrangements for the UK change following the European Union General Data Protection Regulation (GDPR) announced in 2016. This represents a significant shift in legislation and replaces the Data Protection Act 1998. The UK legislation was announced on the 14th September 2017. The Data Protection Bill's (DP Bill) journey through parliament and the associated text has been published online. The EU GDPR gives members states, like the UK, limited opportunities to make unique provision for how the regulation applies. However, the GDPR and the DP Bill should not be considered separately from each other.

In December 2020, EU GDPR was replaced with UK-GDPR. The key principles, rights and obligations remain the same. However, there are implications for the rules on transfers of personal data between the UK and the EEA.

The UK GDPR also applies to controllers and processors based outside the UK if their processing activities relate to:

- offering goods or services to individuals in the UK; or
- monitoring the behaviour of individuals taking place in the UK.

There are also implications for UK controllers who have an establishment in the EEA, have customers in the EEA, or monitor individuals in the EEA. The EU GDPR still applies to this processing, but the way you interact with European data protection authorities has changed.

Are schools in England and Wales required to comply?

In short, yes. Any natural or legal person, public authority, agency or other body which processes personal data is considered a 'data controller'. Given the nature of schools and the personal data required in a variety of forms to operate a Schools this means that an educational college in the UK is required to comply.

Guidance for schools is available on the Information Commissioner's Office website including information about the new regulations.

Freedom of Information Act

All schools (including Academies, which were previously exempt) must have a Freedom of Information Policy which sets out how it will deal with FOI requests. Good advice would encourage the school to:

- Delegate to the Headteacher day-to-day responsibility for FOI policy and the provision of advice, guidance, publicity and interpretation of the school's policy
- Consider designating an individual with responsibility for FOI, to provide a single point of reference, coordinate FOI and related policies and procedures, take a view on possibly sensitive areas and consider what information and training staff may need
- Consider arrangements for overseeing access to information and delegation to the appropriate governing body
- Proactively publish information with details of how it can be accessed through a Publication Scheme (see Model Publication Scheme below) and review this annually
- Ensure that a well-managed records management and information system exists in order to comply with requests
- Ensure a record of refusals and reasons for refusals is kept, allowing the school to review its access policy on an annual basis

Model Publication Scheme

The Information Commissioner's Office provides schools and organisations with a model publication scheme which they should complete. The school's publication scheme should be reviewed annually. The ICO produce guidance on the model publication scheme for schools. This is designed to support schools complete the Guide to Information for Schools.

Personal Data

The school and its employees will have access to a wide range of personal information and data. The data may be held in a digital format or on paper records. Personal data is defined as any combination of data

items that identifies an individual and provides specific information about them, their families or circumstances. This will include:

- Personal information about members of the school community – including students / students, members of staff and parents / carers e.g., names, addresses, contact details, legal guardianship contact details, health records, disciplinary records
- Curricular / academic data e.g., class lists, student / student progress records, reports, references
- Professional records e.g., employment history, taxation and national insurance records, appraisal records and references
- Any other information that might be disclosed by parents / carers or by other agencies working with families or staff members.

Fee

The school should pay the relevant fee to the ICO.

Responsibilities

Every maintained school in the UK is required to appoint a Data Protection Officer as a core function of 'the businesses includes:

- regular and systematic monitoring of individuals on a large scale.
- [the processing of] special categories[2] of data on a large scale and data relating to criminal convictions and offences

The Data Protection Officer (DPO) can be internally or externally appointed.

They must have:

- Expert knowledge
- Timely and proper involvement in all issues relating to data protection
- The necessary resources to fulfil the role
- Access to the necessary personal data processing operations
- A direct reporting route to the highest management level

The data controller must:

- Not give the DPO instructions regarding the performance of tasks
- Ensure that the DPO does not perform a duty or role that would lead to a conflict of interests

[2] • 'Special categories of data' is the type of data which reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; genetic data, biometric data or data concerning health or sex life and sexual orientation

- Not dismiss or penalise the DPO for performing the tasks required of them

As a minimum a Data Protection Officer must:

- Inform, as necessary, the controller, a processor or an employee of their obligations under the data protection laws
- Provide advice on a data protection impact assessment
- Co-operate with the Information Commissioner
- Act as the contact point for the Information Commissioner
- Monitor compliance with policies of the controller in relation to the protection of personal data
- Monitor compliance by the controller with data protection laws

The school may also wish to appoint a Data Manager. Schools are encouraged to separate this role from that of Data Protection Officer, where possible. This person will keep up to date with current legislation and guidance and will:

- determine and take responsibility for the school's information risk policy and risk assessment
- oversee the System Controllers

The school may also wish to appoint System Controllers for the various types of data being held (e.g., student / student information / staff information / assessment data etc.). These Controllers will manage and address risks to the information and will understand:

- what information is held, for how long and for what purpose,
- how information has been amended or added to over time, and
- who has access to the data and why.

Everyone in the school has the responsibility of handling protected or sensitive data in a safe and secure manner.

Governors are required to comply fully with this policy in the event that they have access to personal data, when engaged in their role as a Governor.

Information to Parents / Carers – the Privacy Notice and Consent

In order to comply with the fair processing requirements in data protection law, the school will inform parents / carers of all students / students of the data they collect, process and hold on the students / students, the purposes for which the data is held and the third parties (e.g., LA, DfE, etc.) to whom it may be passed. This privacy notice will be passed to parents / carers for example in the prospectus,

newsletters, reports or a specific letter / communication. Parents / carers of young people who are new to the school will be provided with the privacy notice through an appropriate mechanism.

More information about the suggested wording of privacy notices can be found on the DfE website.

The DFE only publishes documents for England. But these template privacy notices may be suitable for amendment by schools in other UK nations.

Consent under the regulation has changed. Consent is defined as:

"In relation to the processing of personal data relating to an individual, means a freely given, specific, informed and unambiguous indication of the individual's wishes by which the individual, by a statement or by a clear affirmative action, signifies agreement to the processing of the personal data"

This means that where a school is relying on consent as the basis for processing personal data that consent has to be clear, meaning that pre-ticked boxes, opt-out or implied consent are no longer suitable. Students / students aged 13 or over (the age proposed in the Data Protection Bill, subject to Parliamentary approval) may be able to consent to their data being processed for the purposes of information society services. The GDPR does not specify an age of consent for general processing bur schools should consider the capacity of students / students to freely give their informed consent.

Schools should satisfy themselves that their consent forms are clear and written in plain language. Consent should also detail in a very clear and specific way why this is necessary, what will happen to the data, and, how and when it will be disposed of.

Consent is just one of the six lawful bases for processing data:

1. Consent:
2. Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
3. Legal obligation: the processing is necessary for you to comply with the law
4. Vital interests: the processing is necessary to protect someone's life.
5. Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
6. Legitimate interests: processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. (This cannot apply if you are a public authority processing data to perform your official tasks.)

Previously maintained schools were able to rely on the 'legitimate interests' justification. But under the new laws, this has been removed for Public Bodies (which includes schools as defined in Schedule 1 of the Freedom of Information Act 2000 and referenced in the UK Data Protection Bill 2017). This now means that should you wish to process the personal data of a child a risk assessment must be completed, and justification documented.

Parental permission for use of cloud hosted services

Schools that use cloud hosting services are advised to seek appropriate consent to set up an account for students / students.

Data Protection Impact Assessments (DPIA)

According to the ICO, Data Protection Impact Assessments (DPIA): "help organisations to identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy."

These will be carried out by Data Managers under the support and guidance of the DPO. These are intended to be carried out before processing activity starts, although some may need to be retrospective in the early stages of compliance activity.

The risk assessment will involve:

- Recognising the risks that are present
- Judging the level of the risks (both the likelihood and consequences)
- Prioritising the risks.

According to the ICO a DPIA should contain:

- A description of the processing operations and the purpose.
- An assessment of the necessity and proportionality of the processing in relation to the purpose.
- An assessment of the risks to individuals.
- The measures in place to address risk, including security and to demonstrate that you comply.

Or more simply and fully:

- Who did you talk to about this?
- What is going to happen with the data and how – collection, storage, usage, disposal
- How much personal data will be handled (number of subjects)
- Why you need use personal data in this way
- What personal data (including if it's in a 'special category') are you using
- At what points could the data become vulnerable to a breach (loss, stolen, malicious)

- What are the risks to the rights of the individuals if the data was breached
- What are you going to do in order to reduce the risks of data loss and prove you are compliant with the law?

DPIA is an ongoing process and should be re-visited at least annually to verify that nothing has changed since the processing activity started.

Special categories of personal data

The following list is a list of personal data listed in the GDPR as a 'special category'.
"Revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation"

In order to lawfully process special category data, you must identify both a lawful basis and a separate condition for processing special category data. You should decide and document this before you start processing the data.

Use of Biometric Information

The Protection of Freedoms Act 2012, included measures that affect schools that use biometric recognition systems, such as fingerprint identification and facial scanning:

- For all students in schools under 18, they must obtain the written consent of a parent before they take and process their child's biometric data
- They must treat the data with appropriate care and must comply with data protection principles as set out in the Data Protection Act
- They must provide alternative means for accessing services where a parent or student has refused consent

New advice to schools makes it clear that they are not able to use students' biometric data without parental consent. Schools may wish to incorporate the parental permission procedures into revised consent processes.

Training & awareness

All staff must receive data handling awareness / data protection training and will be made aware of their responsibilities, through opportunities such as:

- Induction training for new staff

- Staff meetings / briefings / INSET
- Day to day support and guidance from System Controllers

Secure storage of and access to data

The school should ensure that systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them. Access to protected data will be controlled according to the role of the user. Members of staff will not, as a matter of course, be granted access to the whole management information system.

Good practice suggests that all users will use strong passwords made up from a combination of simpler words. User passwords must never be shared and MfA should be used where possible.

Personal data may only be accessed on machines that are securely protected. Any device that can be used to access personal data must be locked if left (even for very short periods) and set to auto lock if not used for five minutes.

All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.

Personal data should only be stored on school equipment. Private equipment (i.e., owned by the users) must not be used for the storage of school personal data.

When personal data is stored on any portable computer system, USB stick or any other removable media:

- the data must be encrypted, and password protected,
- the device must be password protected
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete.

The school will need to set its own policy as to whether data storage on removal media is allowed, even if encrypted. Some organisations do not allow storage of personal data on removable devices.

The school should have a clear policy and procedures for the automatic backing up, accessing and restoring all data held on school systems, including off-site backups.

The school should have clear policy and procedures for the use of "Cloud Based Storage Systems" (for example Dropbox, Microsoft 365, Google drive) and is aware that data held in remote and cloud storage is still required to be protected in line with the Data Protection Act. The school will ensure that it is satisfied

with controls put in place by remote / cloud-based data services providers to protect the data. The ICO produced guidance about cloud storage for organisations in 2012.

As a Data Controller, the school is responsible for the security of any data passed to a "third party". Data Protection clauses must be included in all contracts where personal data is likely to be passed to a third party.

All paper based personal data must be held in lockable storage, whether on or off site.

Subject Access Requests

Data subjects have a number of rights in connection with their personal data:

- Right to be informed – Privacy notices
- Right of access – Subject Access Request
- Right to rectification – correcting errors
- Right to erasure – deletion of data when there is no compelling reason to keep it
- Right to restrict processing – blocking or suppression of processing
- Right to portability – Unlikely to be used in a school context
- Right to object – objection based on grounds pertaining to their situation
- Rights related to automated decision making, including profiling

Clearly several of these have the opportunity to impact on schools, one being the right of access. Procedures must be in place to deal with Subject Access Requests i.e., a written request to see all or a part of the personal data held by the data controller in connection with the data subject. Data subjects have the right to know: if the data controller holds personal data about them; a description of that data; the purpose for which the data is processed; the sources of that data; to whom the data may be disclosed; and a copy of all the personal data that is held about them. The school must provide the information free of charge, however a 'reasonable fee' may be charged where the request is manifestly unfounded or excessive, especially if this is a repetitive request. See later information on Records of Processing Activity.

Secure transfer of data and access out of school

The school recognises that personal data may be accessed by users out of school or transferred to the LA or other agencies. In these circumstances:

- Users may not remove or copy sensitive or restricted or protected personal data from the school or authorised premises without permission and unless the media is encrypted, and password protected and is transported securely for storage in a secure location

- Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (e.g., family members) when out of school
- When restricted or protected personal data is required by an authorised user from outside the organisation's premises (for example, by a member of staff to work from their home), they should preferably have secure remote access to the management information system or learning platform
- If secure remote access is not possible, users must only remove or copy personal or sensitive data from the organisation or authorised premises if the storage media, portable or mobile device is encrypted and is transported securely for storage in a secure location
- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software
- Particular care should be taken if data is taken or transferred to another country, particularly outside Europe, and advice should be taken from the local authority (if relevant) in this event.

Disposal of data

The school should implement a document retention schedule that defines the length of time data is held before secure destruction. The Information and Records Management Society Toolkit for schools provide support for this process. The school must ensure the safe destruction of personal data when it is no longer required.

The disposal of personal data, in either paper or electronic form, must be conducted in a way that makes reconstruction highly unlikely. Electronic files must be securely disposed of, and other media must be shredded, incinerated or otherwise disintegrated.

A Destruction Log should be kept of all data that is disposed of. The log should include the document ID, classification, date of destruction, method and authorisation.

Audit Logging / Reporting / Incident Handling

Organisations are required to keep records of processing activity. This must include:

- The name and contact details of the data controller
- Where applicable, the name and contact details of the joint controller and data protection officer
- The purpose of the processing
- To whom the data has been/will be disclosed
- Description of data subject and personal data
- Where relevant the countries it has been transferred to
- Under which condition for processing the data has been collected
- Under what lawful basis processing is being carried out

- Where necessary, how it is retained and destroyed
- A general description of the technical and organisational security measures.

Clearly, in order to maintain these records good auditing processes must be followed, both at the start of the exercise and on-going throughout the lifetime of the requirement. Therefore, audit logs will need to be kept to:

- provide evidence of the processing activity and the DPIA
- record where, how and to whom data has been shared
- log the disposal and destruction of the data
- enable the school to target training at the most at-risk data
- record any breaches that impact on the data

It then follows that in the event of a data breach, the school/ college should have a policy for reporting, managing and recovering from information risk incidents, which establishes:

- a "responsible person" for each incident
- a communications plan, including escalation procedure
- and results in a plan of action for rapid resolution
- a plan of action of non-recurrence and further awareness raising

All significant data protection incidents must be reported through the DPO to the Information Commissioner's Office based upon the local incident handling policy and communication plan. The new laws require that this notification should take place within 72 hours of the breach being detected, where feasible.

Data Mapping

The process of data mapping is designed to help schools identify with whom their data is being shared in order that the appropriate contractual arrangements can be implemented. If a third party is processing personal data on your behalf about your students, then this processor has obligations on behalf of the school to ensure that processing takes place in compliance with data protection laws.

Privacy and Electronic Communications

Schools should be aware that they are subject to the Privacy and Electronic Communications Regulations in the operation of their websites.

Millais School

Online Safety Policy

Links to Other Organisations or Documents

Links to other organisations or documents

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/
Southwest Grid for Learning - https://swgfl.org.uk/products-services/online-safety/
Childnet – http://www.childnet-int.org/
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 Child Internet Safety (UKCCIS) - www.education.gov.uk/ukccis
Netsmartz - http://www.netsmartz.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 - Better relationships, better learning, better 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

UKSIC - Safety Features on Social Networks

Children's Commissioner, TES and Schillings – Young peoples' rights on social media

Curriculum

SWGfL Digital Literacy & Citizenship curriculum

UKCCIS – Education for a connected world framework

Teach Today – www.teachtoday.eu/

Insafe - Education Resources

Mobile Devices / BYOD

Cloudlearn Report Effective practice for schools moving to end locking and blocking

NEN - Guidance Note - BYOD

Data Protection

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

ICO Guide for Organisations (general information about Data Protection)

ICO Guides for Education (wide range of sector specific guides)

DfE advice on Cloud software services and the Data Protection Act

ICO Guidance on Bring Your Own Device

ICO Guidance on Cloud Computing

ICO - Guidance we gave to schools - September 2012

IRMS - Records Management Toolkit for Schools

NHS - Caldicott Principles (information that must be released)

ICO Guidance on taking photos in schools

Dotkumo - Best practice guide to using photos

Professional Standards / Staff Training

DfE – Keeping Children Safe in Education

DfE - Safer Working Practice for Adults who Work with Children and Young People

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 - resources for parents workshops / education

The Digital Universe of Your Children - animated videos for parents (Insafe)

Cerebra - Learning Disabilities, Autism and Internet Safety - a Parents' Guide

Insafe - A guide for parents - education and the new media

Research

EU Kids on Line Report - "Risks and Safety on the Internet" - January 2011

Futurelab - "Digital participation - its not chalk and talk any more!"

Ofcom –Media Literacy Research

Millais School

Online Safety Policy

Glossary of Terms

Glossary of Terms

AUP / AUA	Acceptable Use Policy / Agreement – see templates earlier in this document
CEOP	Child Exploitation and Online Protection Centre (part of UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes.
CPD	Continuous Professional Development
FOSI	Family Online Safety Institute
ICO	Information Commissioners Office
ICT	Information and Communications Technology
ICTMark	Quality standard for schools provided by NAACE
INSET	In Service Education and Training
IP address	The label that identifies each computer to other computers using the IP (internet protocol)
ISP	Internet Service Provider
ISPA	Internet Service Providers' Association
IWF	Internet Watch Foundation
LA	Local Authority
LAN	Local Area Network
MIS	Management Information System
MfA	Multi-factor Authentication
NEN	National Education Network – works with the Regional Broadband Consortia (e.g. SWGfL) to provide the safe broadband provision to schools across Britain.
Ofcom	Office of Communications (Independent communications sector regulator)

SWGfL	South West Grid for Learning Trust – the Regional Broadband Consortium of SW Local Authorities – is the provider of broadband and other services for schools and other organisations in the SW
TUK	Think U Know – educational online safety programmes for schools, young people and parents.
VLE	Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting,
WAP	Wireless Application Protocol
UKSIC	UK Safer Internet Centre – EU funded centre. Main partners are SWGfL, Childnet and Internet Watch Foundation.