MILFORD INFANTS
Church Road, Milford
Godalming GU8 5JA

Grow, Learn, Believe, Achieve

ESafety
and
Data Security

Guidance Policies for ICT Acceptable Use

Date of issue: November 2018

Review date: November 2020

Contents

1. Introduction and Overview

Rationale
The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at Milford School with respect to the use of ICT-based technologies.
- Safeguard and protect the children and staff of Milford School
- Assist school staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the internet for educational, personal or recreational use.
- Have clear structures to deal with online abuse such as cyberbullying which are cross referenced with other school policies.
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Minimise the risk of misplaced or malicious allegations made against adults who work with students.

The main areas of risk for our school community can be summarised as follows:
Content

- Exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse
- Lifestyle websites, for example pro-anorexia/self-harm/suicide sites
- Hate sites
- Content validation: how to check authenticity and accuracy of online content

Contact

- Grooming
- Cyber-bullying in all forms
- Identity theft (including 'frape' (hacking Facebook profiles)) and sharing passwords, and the creation of bogus accounts.

Conduct

- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and well-being (amount of time spent online (internet or gaming))
- Sexting (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images)
- Copyright (care or consideration for intellectual property and ownership – such as music and film) (Ref Ofsted 2013)

Schools hold personal data on learners, staff and other people to help them conduct their day to day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in media coverage, and potentially damage the reputation of the school. This can make it difficult for a school to use technology to benefit learners.

Everybody in the school has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

Scope (from SWGfL)

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

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the *school* site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

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 e-safety behaviour that take place out of school.

Both this policy and the Acceptable Use Agreements for all staff, governors, visitors and pupils are inclusive of both fixed and mobile internet technologies provided by the school and technologies owned by pupils and staff but brought onto school premises.

Role	Key Responsibilities
Headteacher	● To take overall responsibility for e-Safety provision ● To take overall responsibility for data and data security (SIRO) ● To ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements ● To be responsible for ensuring that staff receive suitable training to carry out their e-safety roles and to train other colleagues, as relevant ● To be aware of procedures to be followed in the event of a serious e-Safety incident. ● To receive regular monitoring reports from the E-Safety Co-ordinator / Officer ● To ensure that there is a system in place to monitor and support staff who carry out internal e-safety procedures (e.g. network manager)

e-Safety Co-ordinator / Designated Child Protection Lead	● takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents ● promotes an awareness and commitment to e-safeguarding throughout the school community ● ensures that e-safety education is embedded across the curriculum ● liaises with school ICT technical staff ● To communicate regularly with SLT and the designated e-Safety Governor / committee to discuss current issues, review incident logs and filtering / change control logs ● To ensure that all staff are aware of the procedures that need to be followed in the event of an e-Safety incident ● To ensure that an e-Safety incident log is kept up to date ● facilitates training and advice for all staff ● liaises with the Local Authority and relevant agencies ● Is regularly updated in e-safety issues and legislation, and be aware of the potential for serious child protection 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 • cyber-bullying and use of social media
Governors / E-safety governor	● To ensure that the school follows all current e-Safety advice to keep the children and staff safe ● To approve the E-Safety Policy and review the effectiveness of the policy. This will be carried out by the Governors / Governors Sub Committee receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of E-Safety Governor ● To support the school in encouraging parents and the wider community to become engaged in e-safety activities ● The role of the E-Safety Governor will include: • regular review with the E-Safety Co-ordinator / Officer (including e-safety incident logs, filtering / change control logs)
Computing Curriculum Leader	● To oversee the delivery of the e-safety element of the Computing curriculum ● To liaise with the e-safety coordinator regularly ● To support Governors and School in the education of parents in relation to internet safety.

Network Manager/technician	● To report any e-Safety related issues that arises, to the e-Safety coordinator. ● To ensure that users may only access the school's networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed ● To ensure that provision exists for misuse detection and malicious attack e.g. keeping virus protection up to date ● To ensure the security of the school ICT system ● To ensure that access controls exist to protect personal and sensitive information held on school-owned devices (only certain users have access to admin server) • the school's policy on web filtering is applied and updated on a regular basis • that he / she keeps up to date with the school's e-safety policy and technical information in order to effectively carry out their e-safety role and to inform and update others as relevant • that the use of the *network* / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher for investigation / action / sanction ● To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster. ● To keep up-to-date documentation of the school's e-security and technical procedures – use help desk log
Data Manager (School Business Manager)	● To ensure that all data held on pupils on the school office machines have appropriate access controls in place
Teachers	● To embed e-safety issues in all aspects of the curriculum and other school activities ● To supervise and guide pupils carefully when engaged in learning activities involving online technology (including extra-curricular and extended school activities if relevant) ● To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws
All staff	● To read, understand and help promote the school's e-Safety policies and guidance ● To read, understand, sign and adhere to the school staff Acceptable Use Agreement / Policy ● To be aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices ● To report any suspected misuse or problem to the e-Safety coordinator ● To maintain an awareness of current e-Safety issues and guidance e.g. through CPD ● To model safe, responsible and professional behaviours in their own use of technology ● To ensure that any digital communications with pupils should be on a professional level and only through school based systems, never

	through personal mechanisms, e.g. email, text, mobile phones etc.
Pupils	● Read, understand, sign and adhere to the Student / Pupil Acceptable Use Policy (nb. In EYFS and KS1 it would be expected that parents / carers would sign on behalf of the pupils) ● have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations ● to understand the importance of reporting abuse, misuse or access to inappropriate materials ● to know what action to take if they or someone they know feels worried or vulnerable when using online technology. ● to know and understand school policy on the use of mobile phones, digital cameras and hand held devices. ● To know and understand school policy on the taking / use of images and on cyber-bullying. ● To understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school ● To take responsibility for learning about the benefits and risks of using the internet and other technologies safely both in school and at home ● to help the school in the creation/ review of e-safety policies
IT and Computing Curriculum Lead	● Maintain the integrity of the software required to deliver the curriculum ● Educating Parents and raising awareness as instructed by Head ● Check any websites or software as requested by the teaching staff prior to allowing access to it through the filter.
Parents/carers	● to support the school in promoting e-safety and endorse the Parents' Acceptable Use Agreement which includes the pupils' use of the internet and the school's use of photographic and video images ● to read, understand and promote the school Pupil Acceptable Use Agreement with their children ● to access the school website / Google Classroom / on-line student / pupil records in accordance with the relevant school Acceptable Use Agreement. ● to consult with the school if they have any concerns about their children's use of technology
External groups	● Any external individual / organisation will sign an Acceptable Use Policy prior to using any equipment or the internet within school

Communication:
The policy will be communicated to staff/pupils/community in the following ways:

- Policy to be posted on the school website/ staffroom/ classrooms
- Policy to be part of school induction pack for new staff
- Acceptable use agreements discussed with pupils at the start of each year.
- Acceptable use agreements to be issued to whole school community, usually on entry to the school
- Acceptable use agreements to be held in pupil and personnel files

Handling complaints:

- The school will take all reasonable precautions to ensure e-Safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.

- Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:

    - informing parents or carers;
    - removal of Internet or computer access for a period,
    - referral to LA / Police.

- Our e-Safety Coordinator acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher.

- Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school / LA child protection procedures.

Review and Monitoring

The e-safety policy is referenced from within other school policies: ICT and Computing policy, Child Protection policy, Anti-Bullying policy and in the School Development Plan, Behaviour policy, Personal, Social and Health Education and for Citizenship policies .

- The school has an e-safety coordinator who will be responsible for document ownership, review and updates.
- The e-safety policy will be reviewed bi-annually or when any significant changes occur with regard to the technologies in use within the school
- The e-safety policy has been written by the school e-safety Coordinator and is current and appropriate for its intended audience and purpose.
- There is widespread ownership of the policy and it has been agreed by the SLT and approved by Governors and other stakeholders such as the PTA. All amendments to the school E -Safeguarding policy will be discussed in detail with all members of teaching staff.

2. Education and Curriculum

Pupil e-Safety curriculum

This school

- Has a clear, progressive e-safety education programme as part of the Computing curriculum / PSHE curriculum. It is built on LA e-Safeguarding and e-literacy framework for EYFS to Y2/ national guidance. This covers a range of skills and behaviours appropriate to their age and experience, including:
    - to STOP and THINK before they CLICK
    - to develop a range of strategies to evaluate and verify information before accepting its accuracy;
    - to be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be;
    - to know how to narrow down or refine a search;
    - [for older pupils] to understand how search engines work and to understand that this affects the results they see at the top of the listings;
    - to understand acceptable behaviour when using an online environment / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private;
    - to understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
    - to understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments;
    - to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings;
    - to understand why they must not post pictures or videos of others without their permission;
    - to know not to download any files – such as music files - without permission;
    - to have strategies for dealing with receipt of inappropriate materials;
    - [for older pupils] to understand why and how some people will 'groom' young people for sexual reasons;
    - To understand the impact of cyberbullying, sexting and trolling and know how to seek help if they are affected by any form of online bullying.
    - To know how to report any abuse including cyberbullying; and how to to seek help if they experience problems when using the internet and related technologies, i.e. parent or carer, teacher or trusted staff member, or an organisation such as Childline or the CLICK CEOP button.

- Plans internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- Will remind students about their responsibilities through an end-user Acceptable Use Policy which every student will sign.
- Ensures staff will model safe and responsible behaviour in their own use of technology during lessons.
- Ensures that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright / intellectual property rights;

- Ensures that staff and pupils understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include, risks in pop-ups; buying on-line; on-line gaming / gambling;

Staff and governor training

This school

- Ensures staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection;
- Makes regular training available to staff on e-safety issues and the school's e-safety education program to be updated annually.
- Provides, as part of the induction process, all new staff [including those on university/college placement and work experience] with information and guidance on the e-Safeguarding policy and the school's Acceptable Use Policies.

Parent awareness and training

This school

- Runs a rolling programme of advice, guidance and training for parents, including:
    - Introduction of the Acceptable Use Agreements to new parents, to ensure that principles of e-safe behaviour are made clear
    - Information leaflets; in school newsletters; on the school web site; (As development of website continues, provision will be made to access resources via these mediums. In addition we will cover any changes in technology, updating the information available as and when relevant.)
    - demonstrations, practical sessions held at school;
    - suggestions for safe Internet use at home; (Provide parents with Literature supported by Charities)
    - provision of information about national support sites for parents.

3. Expected Conduct and Incident management

Expected conduct

In this school, all users:

- are responsible for using the school ICT systems in accordance with the relevant Acceptable Use Policy which they will be expected to sign before being given access to school systems. (at KS1 it would be expected that parents/carers would sign on behalf of the pupils.)
- need to understand the importance of misuse or access to inappropriate materials and are aware of the consequences
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school

- will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying

Staff
- are responsible for reading the school's e-safety policy and using the school ICT systems accordingly, including the use of mobile phones, and hand held devices.

Students/Pupils
- should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

Parents/Carers
- should provide consent for pupils to use the Internet, as well as other technologies, as part of the e-safety acceptable use agreement form at time of their child's entry to the school
- should know and understand what the 'rules of appropriate use' are and what sanctions result from misuse

Incident Management

In this school:
- there is strict monitoring and application of the e-safety policy and a differentiated and appropriate range of sanctions, though the attitudes and behaviour of users are generally positive and there is rarely need to apply sanctions
- all members and its wider community are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes.
- support is actively sought from other agencies as needed (eg the local authority and regional broadband grid, UK Safer Internet Centre helpline) in dealing with e-safety issues
- monitoring and reporting of e safety incidents takes place and contribute to developments in policy and practice in e-safety within the school. The records are reviewed/audited and reported to the school's senior leaders, Governors /the LA
- parents / carers are specifically informed of e-safety incidents involving young people for whom they are responsible.
- We will contact the Police if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law

4. Managing the ICT infrastructure

- **Internet access, security (virus protection) and filtering**

This school:

- Has an educational filter/secure broadband service provided through RM Unify/RM Safety Net
- Uses a RM Safety Net filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature etc
- Ensures network healthy through use of ESet anti-virus software etc and network set-up so staff and pupils cannot download executable files;
- Uses Egress, Office365 to send personal data over the Internet and uses secure remote access were staff need to access personal level data off-site;
- Blocks all Chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform;
- Has blocked pupil access to music download or shopping sites – except those approved for educational purposes at a regional or national level, such as Audio Network;
- Works in partnership with the LA to ensure any concerns about the system are communicated so that systems remain robust and protect students;
- Is vigilant in its supervision of pupils' use at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access;
- Ensures all staff and students have signed an acceptable use agreement form and understands that they must report any concerns;
- Ensures pupils only publish within an appropriately secure environment : the school's learning environment etc
- Requires staff to preview websites before use [where not previously viewed or cached] Plans the curriculum context for Internet use to match pupils' ability, using child-friendly search engines where more open Internet searching is required; eg yahoo for kids or ask for kids , Google Safe Search , …..
- Never allows 'raw' image search with pupils e.g. Google image search
- Informs all users that Internet use is monitored;
- Informs staff and students that that they must report any failure of the filtering systems directly to the [*teacher / School Business Manager]*. Our system administrator(s) logs or escalates as appropriate to the Technical service provider as necessary;
- Makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse – through staff meetings and teaching programme;
- Provides advice and information on reporting offensive materials, abuse/ bullying etc available for pupils, staff and parents

- Immediately refers any material we suspect is illegal to the appropriate authorities – Police – and the LA.
- Adheres to and keeps abreast of all current legislation and Government policy.

- **Network management (user access, backup)**
  This school
  - Uses individual, audited log-ins for all users;
  - *Has additional local network auditing software installed;*
  - Ensures the Systems Administrator / network manager is up-to-date with LA services and policies / requires the Technical Support Provider to be up-to-date with LA services and policies;
  - Storage of all data within the school will conform to the UK data protection requirements

    Pupils and Staff using mobile technology, where storage of data is online, will conform to the EU GDPR regulations where storage is hosted within the EU.

To ensure the network is used safely, this school:

- Ensures staff read and sign that they have understood the school's e-safety Policy. Following this, they are set-up with Internet, email access and network access. Online access to service is through a unique, audited username and password. We also *provide a different / use the same username and password* for access to our school's network;
- Staff access to the schools' management information system is controlled through a separate password for data security purposes;
- We provide pupils with an individual network log-in username. From Year 1 they are also expected to use a personal password;
- All pupils have their own unique username and password which gives them access to the Internet
- Makes clear that no one should log on as another user and makes clear that pupils should never be allowed to log-on or use teacher and staff logins as these have far less security restrictions and inappropriate use could damage files or the network;
- Has set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas;
- Requires all users to always log off when they have finished working or are leaving the computer unattended;
- Where a user finds a logged-on machine, we require them to always log-off and then log-on again as themselves. [Users needing access to secure data are timed out after 15 mins and have to re-enter their username and password to re-enter the network.];
- Has set-up the network so that users cannot download executable files / programmes;
- Has blocked access to music/media download or shopping sites – except those approved for educational purposes;

- Scans all school mobile equipment with anti-virus / spyware before it is connected to the network;
- Makes clear that staff are responsible for ensuring that all school equipment that goes home has the anti-virus and spyware software maintained up-to-date and the school provides them with a solution to do so;- scanned every time a machine boots up – Pete checks reports from Server each week.
- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used solely to support their professional responsibilities and that they notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- Makes clear that staff accessing LA systems do so in accordance with any Corporate policies;
  e.g. Borough email or Intranet; finance system, Personnel system etc
- Maintains equipment to ensure Health and Safety is followed;
  e.g. projector filters cleaned by site manager / TA; equipment installed and checked by approved Suppliers / LA electrical engineers
- Has integrated curriculum and administration networks, but access to the Management Information System is set-up so as to ensure staff users can only access modules related to their role;
  e.g. teachers access report writing module; SEN coordinator - SEN data;
- Ensures that access to the school's network resources from remote locations by staff is restricted and access is only through school / LA approved systems:
  e.g. teachers access their area / a staff shared area for planning documentation
- Does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is restricted and is only through approved systems;
  e.g. technical support or MIS Support, our Education Welfare Officers accessing attendance data on specific children, parents using a secure portal to access information on their child
- Makes clear responsibilities for the daily back up of MIS and finance systems and other important files;
- Has a clear disaster recovery system in place for critical data that includes a secure, remote back up of critical data, that complies with external Audit's requirements;
- Uses the DfE secure s2s website for all CTF files sent to other schools;
- Ensures that all pupil level data or personal data sent over the Internet is encrypted or only sent within the approved secure system in our LA or through USO secure file exchange (USO FX);
- Follows ISP advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network;
- Our wireless network has been secured to industry standard Enterprise security level /appropriate standards suitable for educational use;
- All computer equipment is installed professionally and meets health and safety standards;
- Projectors are maintained so that the quality of presentation remains high;

- Reviews the school ICT systems regularly with regard to health and safety and security.

Passwords policy

- This school makes it clear that staff and pupils must always keep their password private, must not share it with others and must not leave it where others can find.
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password private.
- We require staff to use STRONG passwords for access into our MIS system.

E-mail

This school

- Provides staff with an email account for their professional use, rmunify and makes clear personal email should be through a separate account;
- Provides highly restricted / simulated environments to show Key Stage 1 pupils email. (Via Purplemash)
- Does not publish personal e-mail addresses of pupils or staff on the school website. We use anonymous or group e-mail addresses, for example info@milford.surrey.sch.uk / head@milford.surrey.sch.uk or class e-mail addresses (with one or more staff having access to an aliased/shared mailbox for a class) for communication with the wider public.
- Will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law.
- Will ensure that email accounts are maintained and up to date
- Reports messages relating to or in support of illegal activities to the relevant Authority and if necessary to the Police.
- Knows that spam, phishing and virus attachments can make e mails dangerous. We use a number of technologies to help protect users and systems in the school, including desktop anti-virus product Sophos, plus direct email filtering for viruses, Trojans, pornography, phishing and inappropriate language.

Pupils:

- Pupils are introduced to, and use e-mail as part of the ICT/Computing scheme of work using PurpleMash.
- Year R/1 pupils are introduced to principles of e-mail through play and closed protected email set up as above.
- Pupils are taught about the safety and 'netiquette' of using e-mail both in school and at home i.e. they are taught:
    - not to give out their e-mail address unless it is part of a school managed project or to someone they know and trust and is approved by their teacher or parent/carer;
    - that an e-mail is a form of publishing where the message should be clear, short and concise;

- that any e-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper;
- they must not reveal private details of themselves or others in email, such as address, telephone number, etc;
- to 'Stop and Think Before They Click' and not open attachments unless sure the source is safe;
- that they should think carefully before sending any attachments;
- embedding adverts is not allowed;
- that they must immediately tell a teacher / responsible adult if they receive an e-mail which makes them feel uncomfortable, is offensive or bullying in nature;
- not to respond to malicious or threatening messages;
- not to delete malicious of threatening e-mails, but to keep them as evidence of bullying;
- not to arrange to meet anyone they meet through e-mail without having discussed with an adult and taking a responsible adult with them;
- that forwarding 'chain' e-mail letters is not permitted.

Staff:

- Staff only use school e-mail systems for professional purposes
- Access in school to external personal e mail accounts may be blocked
- Staff know that e-mail sent to an external organisation must be written carefully, (and may require authorisation), in the same way as a letter written on school headed paper. That it should follow the school 'house-style':
  - the sending of multiple or large attachments should be limited, and may also be restricted by the provider of the service being used;
  - the sending of chain letters is not permitted;
  - embedding adverts is not allowed;
- All staff sign our School Agreement Form to say they have read and understood the e-safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

School website

- The Headteacher takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;
- Uploading of information is restricted to our website authorisers: EG: Headteacher, School Business Manager and Authorised Administration Staff
- The school web site complies with the statutory DfE guidelines for publications;
- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status;
- The point of contact on the web site is the school address, telephone number and we use a general email contact address, e.g. info@stjosephsguildford.com or info@milford.surrey.sch.uk. Home information or individual e-mail identities will not be published;
- Photographs published on the web do not have full names attached;

- We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website;
- We do not use embedded geodata in respect of stored images
- We expect teachers using' school approved blogs or wikis to password protect them and run from the school website.

Learning platform/website

- Uploading of information on the schools' Learning Platform / website space is shared between different staff members according to their responsibilities e.g. all class teachers can upload information in their class areas;
- In school, pupils are only able to upload and publish within school approved and closed systems, such as Purple Mash.

Social networking

- Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the schools' preferred system for such communications.
- As we are a school at Infant level we have taken the view that access to social networking sites is not required and have blocked them via our filter

School staff will ensure that in private use:

- No reference should be made in social media to students / pupils, 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 Milford School or the local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information
- Visitors to the school are requested not to access social networking sites whilst on the premises or use personal devices.
-

Video Conferencing

This school

- Currently N/A

CCTV

- Currently N/A

5. Data security: Management Information System access and Data transfer

Strategic and operational practices

At this school:

- The School Business Manager is the School Data Controller, with Elaine Coward being our Data Protection Officer (DPO).
- Staff are clear who are the key contact(s) for key school information (the Information Asset Owners) are.
- We ensure staff know who to report any incidents where data protection may have been compromised.
- All staff are DBS checked and records are held in one central record

  We ensure ALL the following school stakeholders sign an Acceptable Use Agreement form. We have a system so we know who has signed.

  - staff,
  - governors,
  - pupils
  - parents

  This makes clear staffs' responsibilities with regard to data security, passwords and access.
- We follow LA guidelines for the transfer of any data, such as MIS data or reports of children, to professionals working in the Local Authority or their partners in Children's Services / Family Services, Health, Welfare and Social Services.
- We require that any Protect and Restricted material must be encrypted if the material is to be removed from the school and limit such data removal. / We have an approved remote access solution so staff can access sensitive and other data from home, without need to take data home.
- School staff with access to setting-up usernames and passwords for email, network access and Learning Platform access are working within the approved system and follow the security processes required by those systems.
- We ask staff to have undertaken at least annual house-keeping to review, remove and destroy any digital materials and documents which need no longer be stored.

Technical Solutions

- Staff have password protected areas in which to store sensitive documents or photographs
- We require staff to log-out of systems when leaving their computer, but also enforce lock-out after 15 minutes of idle time.
- We use password protected flash drives if any member of staff has to take any sensitive information off site.
- We use the DfE S2S site to securely transfer CTF pupil data files to other schools.
- We use the Pan-London Admissions system (based on USO FX) to transfer admissions data.
- We use the Egress secure data transfer system
- We store any Protect and Restricted written material in lockable storage cabinets in a lockable storage area.
- All servers are in lockable locations and managed by DBS-checked staff.
- Back Up is completed regularly and is stored on a remote hard drive.

- We comply with the WEEE directive on equipment disposal by using an approved or recommended disposal company for disposal of equipment where any protected or restricted data has been held and get a certificate of secure deletion for any server that once contained personal data.
- Portable equipment loaned by the school (for use by staff at home), where used for any protected data, is disposed of through the same procedure.
- Paper based sensitive information is shredded, using cross cut shredder / collected by secure data disposal service.
- We are using secure file deletion software.

6. Equipment and Digital Content

Personal mobile phones and mobile devices

- Mobile phones brought into school are entirely at the staff member, parents' or visitors own risk. The School accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school.
- All visitors are requested to keep their phones on silent.
- The recording, taking and sharing of images, video and audio on any mobile phone is to be avoided; except where it has been explicitly agreed otherwise by the headteacher. Such authorised use is to be monitored and recorded. All mobile phone use is to be open to scrutiny and the headteacher is to be able to withdraw or restrict authorisation for use at any time if it is to be deemed necessary.
- The School reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying. Staff mobiles or hand held devices may be searched at any time as part of routine monitoring.
- Where parents or students need to contact each other during the school day, they should do so only through the School Office telephone. Staff may use their phones during break times. If a staff member is expecting a personal call they may leave their phone with the school office to answer on their behalf, or seek specific permissions to use their phone at other than their break times.
- Mobile phones and personally-owned devices are not permitted to be used in certain areas within the school site, e.g. toilets.
- Mobile phones will not be used during lessons or formal school time unless as part of an approved and directed curriculum-based activity with consent from the headteacher.
- The Bluetooth or similar function of a mobile phone should be switched off at all times and not be used to send images or files to other mobile phones.
- No images or videos should be taken on mobile phones or personally-owned mobile devices without the prior consent of the person or people concerned.

Staff use of personal devices

- Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity.
- Staff will be issued with a school phone where contact with students, parents or carers is required.
- Mobile Phones and personally-owned devices will be switched off or switched to 'silent' mode. Bluetooth communication should be 'hidden' or switched off and mobile phones or personally-owned devices will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances.
- If members of staff have an educational reason to allow children to use mobile phones or a personally-owned device as part of an educational activity then it will only take place when approved by the senior leadership team.
- Staff should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of students and will only use work-provided equipment for this purpose.
- If a member of staff breaches the school policy then disciplinary action may be taken.
- Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting students or parents, then a school mobile phone will be provided and used. In an emergency where a staff member doesn't have access to a school-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes.

Digital images and video
In this school:

- We gain parental / carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter / son joins the school;
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials / DVDs;
- Staff sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones / personal equipment for taking pictures of pupils;
- If specific pupil photos (not group photos) are used on the school web site, in the prospectus or in other high profile publications the school will obtain individual parental or pupil permission for its long term use
- The school blocks/filter access to social networking sites or newsgroups unless there is a specific approved educational purpose;
- Pupils are taught about how images can be manipulated in their e-Safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their Computing scheme of work;

- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identify of others and their location, such as house number, street name or school. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

Asset disposal

Details of all school-owned hardware will be recorded in a hardware inventory.
Details of all school-owned software will be recorded in a software inventory.
All redundant equipment will be disposed of through an authorised agency. This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.
All redundant equipment that may have held personal data will have the storage media forensically wiped. Alternatively, if the storage media has failed, it will be physically destroyed. The school will only use authorised companies who will supply a written guarantee that this will happen
Disposal of any equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website.

Current Legislation

Acts Relating to Monitoring of Staff email

GDPR 2018
The Act requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual. The Act grants individuals rights of access to their personal data, compensation and prevention of processing.

The Telecommunications (Lawful Business Practice)

(Interception of Communications) Regulations 2000
http://www.hmso.gov.uk/si/si2000/20002699.htm

Regulation of Investigatory Powers Act 2000
Regulating the interception of communications and making it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored. Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.

http://www.hmso.gov.uk/acts/acts2000/20000023.htm

Human Rights Act 1998
http://www.hmso.gov.uk/acts/acts1998/19980042.htm

Other Acts Relating to eSafety

Racial and Religious Hatred Act 2006
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.

Sexual Offences Act 2003
The new 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. Schools should already have a copy of "*Children & Families: Safer from Sexual Crime*" document as part of their child protection packs.

For more information www.teachernet.gov.uk

Communications Act 2003 (section 127)
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.

The Computer Misuse Act 1990 (sections 1 – 3)
Regardless of an individual's motivation, the Act makes it a criminal offence to gain:

- access to computer files or software without permission (for example using another persons password to access files)
- unauthorised access, as above, in order to commit a further criminal act (such as fraud)
- impair the operation of a computer or program

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Malicious Communications Act 1988 (section 1)
This legislation makes it a criminal offence to send an electronic message (e-mail) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Copyright, Design and Patents Act 1988
Copyright is the right to prevent others from copying or using work without permission. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer. Copyright infringement is to copy all or a substantial part of anyone's work without obtaining them author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Public Order Act 1986 (sections 17 – 29)
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.

Protection of Children Act 1978 (Section 1)
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 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.

Obscene Publications Act 1959 and 1964
Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

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.

Acts Relating to the Protection of Personal Data

Data Protection Act 2018
www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpga_20180012_en.pdf

The Freedom of Information Act 2000

http://www.ico.gov.uk/for_organisations/freedom_of_information_guide.aspx

Useful Websites:

www.thinkuknow.co.uk/teachers/resources

www.surreycc.gov.uk/people-and-community

www.surreycc.gov.uk/school-and-learning

www.nspcc.org.uk

www.discoveryeducation.co.uk

www.espresso.co.uk

www.gov.uk/government/publications/promoting-fundamental-british-values-through-smsc

Appendices:

1. Acceptable Use Agreement, Staff, Governors and Visitors
2. Acceptable Use Agreements Pupils
3. Acceptable Use Agreement including photo/video permission (Parents)

Staff, Governor and Visitor
Acceptable Use Agreement / Code of Conduct

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents

- Ø I will only use the school's ICT systems for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- Ø I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- Ø I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- Ø I will only use the approved school email system for school business.
- Ø I will ensure that personal data (such as data held on RM Integris) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body.
- Ø I will not install any hardware or software without permission.
- Ø I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Ø Images of pupils and/ or staff will only be taken, stored and used for professional purposes inline with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher.
- Ø I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Headteacher.
- Ø I will respect copyright and intellectual property rights.
- Ø I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- Ø I will support and promote the school's E-Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.

User Signature

I agree to follow this code of conduct and to support the safe use of ICT throughout the school

Signature …….…… Date ……

Full Name …….....(printed)

Job title . . . . . .

Date:

Acceptable Use Agreement : Pupils - KS1 and EYFS Primary

- **I promise** to only use school technology for school work that my teacher has asked me to do
- **I promise** not to look for or show other people things that might make them feel sad.
- **I promise** to be kind to other people online.
- **I will not** use other people's work or pictures unless they say it's ok.
- **I will not** damage the equipment on purpose. If I accidentally damage something I will tell my teacher.
- **I will not** share my password with anybody except my parents or carers. If I forget my password I tell my teacher.
- **I will not** use other people's usernames or passwords.
- **I will not** share personal information online with anyone or arrang**e** to meet someone online.
- **I will not** download anything from the Internet unless my teacher has asked me to.
- **I will** only use my class email address or my own school email address when emailing.
- **I will** only open email attachments and shared files from people I know, or who my teacher has approved.
- **I will** be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- **I will** keep the school esafety rules
- **I will** tell my teacher if anybody asks for personal information.
- **I will** tell my teacher if anybody says or does anything to me that makes me feel sad.
- **I will** be polite to everybody online; I will treat everybody the way that I want to be treated.
- **I understand** that some people on the Internet can be unkind. I will tell my teacher if I am ever worried in school, or my parents if I am at home.
- **I understand** that my use of ICT can be checked and that my parent/ carer can be told if an adult at school is concerned about my esafety**.**
- **I understand** that if I break any of this agreement there will be consequences to my actions and my parent will be informed.

Pupil Name: ……..

Signed (Parent): .....

Signed (Pupil): ……..

Date: ……