KOINONIA

FELLOWSHIP • FAITH • FAMILY

St Mary Magdalene C of E School
with
Christ Church C of E Primary School

E-Safety Policy

This policy was:	Written in	September 2015	
	Updated in	March 2020	
	Review date	Summer 2021	
	Approved by	Dr P Gregory	Mrs J Eastaugh
		Co-Chairs of Governors	
		PGregory	G.P. Eastaugh
		Mrs C Harrison	Mrs V Wainwright
		Federation Co-Headteachers	
		C Harrison.	VHWainwright

Contents

1. Introduction and Overview

IT in the 21st Century has an all-encompassing role within the lives of children, young people and adults. New Internet and online technologies are enhancing communication and the sharing of information.

Current and emerging Internet and online technologies used in school and, more importantly in many cases, used outside of school by children include:

- The Internet – World Wide Web
- E-mail
- Instant messaging (often using simple web cams) e.g. Instant Messenger)
- Web based voice and video calling (e.g. Skype)
- Online chat rooms
- Online discussion forums
- Social networking sites (e.g. Facebook, WhatsApp)
- Blogs and Micro-blogs (e.g. Twitter)
- Podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player)
- Video broadcasting sites (e.g. YouTube)
- Music and video downloading (e.g. iTunes, Spotify)
- Mobile phones with camera and video functionality
- Smart phones with e-mail, messaging and internet access

OUR FEDERATION APPROACH TO THE SAFE USE OF IT

Creating a safe IT learning environment includes three main elements within our Federation:

- An effective range of technological tools;
- Policies and procedures, with clear roles and responsibilities
- E-Safety teaching is embedded into the school curriculum and schemes of work

Rationale and scope
The purpose of this policy is to:

- Set out the key principles expected of all members of the school communities within the Koinonia Federation with respect to the use of ICT-based technologies.
- Safeguard and protect the children and staff within the Koinonia Federation
- 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 cyber-bullying 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 Federation 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 abusive/derogatory language), substance abuse
- Lifestyle websites, for example pro-anorexia/self-harm/suicide sites
- Hate sites including those relating to PREVENT
- Content validation: how to check authenticity and accuracy of online content

Contact

- Grooming (sexual exploitation, radicalisation etc.)
- Online-bullying in all forms
- Social or commercial identity theft, including passwords

Conduct

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

(Ref Ofsted 2013)

Scope

This policy applies to all members of the Koinonia Federation of Schools (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of the Federation's IT systems, both in and out of the Koinonia Federation premises.

The Education and Inspections Act 2006 empowers the Executive Co-Headteachers to such extent as is reasonable, to regulate the behaviour of pupils 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 cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the Federation of schools. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The Federation 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 outside school.

Role	Key Responsibilities
Federation Executive Co-Headteachers/ Campus Leaders	• 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 e.g. Outlook 365 • 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 • 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)
Campus E-Safety Co-ordinator	• 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 IT technical staff • To communicate regularly with SLT and the designated e-safety Governor / committee to discuss current issues, review incident logs and filtering • 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 on e-safety issues and legislation, and is aware of the potential for serious child protection issues to arise from: • the 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 Federation 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 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 Kyla Butterworth

Role	Key Responsibilities
	• To support the Federation in encouraging parents and the wider community to become engaged in e-safety activities • The role of the E-Safety Governor will include: o regular reviews with the E-Safety Co-ordinators at each campus (including e-safety incident logs, filtering / change control logs)
Computing Curriculum Leaders	• To oversee the delivery of the e-safety element of the Computing curriculum • To liaise with the e-safety coordinators regularly
Federation IT Technicians	• To report any e-safety related issues that arise to the e-safety coordinator. • To ensure that users may only access the Federation 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 IT system • To ensure that access controls / encryption exist to protect personal and sensitive information held on school-owned devices • To ensure the Federation's policy on web filtering is applied and updated on a regular basis • To ensure RM is informed of issues relating to the filtering applied by the Grid • To keep up to date with the Federation'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 • To ensure the use of the *network* / *email* is regularly monitored in order that any misuse / attempted misuse can be reported to the *E-Safety Co-ordinator /Campus Leader 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 Federation's e-security and technical procedures
Federation Business Manager	• To ensure that all data held on pupils on the Federation admin offices PCs have appropriate access controls in place
AGAS Data Protection Officer	• To ensure that the Federation is compliant with GDPR regulations and to report any breaches to the ICO.
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 Federation's e-safety policies and guidance • To read, understand, sign and adhere to the Federation staff Acceptable Use Agreement

Role	Key Responsibilities
	• 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 Federation 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 Pupil Acceptable Use Policy (NB: at EYFS/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 Federation policy on the use of mobile phones, MacBook, iPad, digital cameras and hand-held devices. • To know and understand Federation 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 Federation'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 Federation in the creation/ review of e-safety policies
Parents/carers	• To support the Federation in promoting e-safety and endorse the Parents' Acceptable Use Agreement which includes the pupils' use of the Internet and the Federation's use of photographic and video images • To read, understand and promote the school Pupil Acceptable Use Agreement with their children • To access the Federation website in accordance with the relevant school Acceptable Use Agreement. • To consult with the schools 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 our Federation

Communication:

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

- Policy to be posted on the Federation 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 centrally filed

Handling complaints:

- The Federation 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 Federation 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:
  - Discussion with class teacher/ Executive Co-Headteachers/Campus Leaders;
  - Informing parents or carers;
  - Removal of Internet or computer access for a period, [which could ultimately prevent access to files held on the system, including examination coursework];
  - Referral to LA / Police.

- Our E-Safety Co-ordinators acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Campus Leaders in the first instance.

- 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: Child Protection policy, Anti-Bullying policy and in the Federation Improvement Plan, Behaviour policies, and PSHE policies.

- The Federation has a Federation lead on e-safety who will be responsible for the document ownership, review and updates. The DPO will do checks on permission slips etc. and DSLs have responsibility for on-line safety.
- The E-safety policy will be reviewed 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 Federation E-safety Leader 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. All amendments to the Federation e-safeguarding policy will be discussed in detail with all members of teaching staff.

2. Education and Curriculum

Pupil e-safety curriculum

This Federation

- Has a clear, progressive e-safety education programme as part of the Computing curriculum and PSHE curriculum. It is built on LA / e-safeguarding and e-literacy frameworks for EYFS to KS4 as well as 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 foul or derogatory 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 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 pupil about their responsibilities through an end-user Acceptable Use Agreement which every pupil 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 Federation

- 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 Federation's e-safety education program through annual updates, staff meetings etc
- 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 Federation's Acceptable Use Policies.

Parent awareness and training

This Federation

- 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;
    - Demonstrations, practical sessions held at school;
    - Suggestions for safe Internet use at home;
    - Provision of information about national support sites for parents.

3. Expected Conduct and Incident management

Expected conduct

In this Federation 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. (In EYFS 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 Federation'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, MacBook, iPads, 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 Federation's e-safety policy and using the school IT systems accordingly, including the use of mobile phones, and hand-held devices.

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 the 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

Within the Federation:

- There are 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 Federation's escalation processes.
- Support is actively sought from other agencies as needed (e.g. 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 / LSCB
- 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**

The Federation:

- Has the educational filtered secure broadband connectivity through RM Broadband and so connects to the 'private' National Education Network;
- Uses RM SafetyNet system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc. All changes to the filtering policy are logged and only available to staff with the approved 'web filtering management' status;
- Uses USO user-level filtering where relevant, thereby closing down or opening up options appropriate to the age / stage of the students;
- Ensures network and end-point protection through use of Sophos anti-virus software etc. and the network is set-up so staff and pupils cannot download harmful files;
- Uses DfE, LA or Office 365 approved systems such as S2S, USO FX, secured email to send personal data over the Internet and uses encrypted devices or 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;
- Only unblocks other external social networking sites for specific purposes / Internet Literacy lessons;
- Has blocked pupil access to music/media download or shopping sites – except those approved for educational purposes at a regional or national level, such as Audio Network;
- Uses security time-outs on Internet access where practicable / useful;
- Works in partnership with RM 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: Office 365 secure platform, etc.
- Requires staff to preview websites before use [where not previously viewed or cached] and encourages use of the Federation's Learning Platform as a key way to direct students to age / subject appropriate web sites; Plans the curriculum context for Internet use to match pupils' ability, using child-friendly search engines where more open Internet searching is required; e.g. Yahoo for Kids or Ask for Kids, Google Safe Search
- Never allows / is vigilant when conducting 'raw' image search with pupils e.g. Google image search;
- Informs all users that Internet use is monitored;
- Informs staff and students that they must report any failure of the filtering systems directly to the e-safety lead who will report to any member of the IT Team with

the IT Manger having overall responsibility. Our system administrator(s) logs or escalates as appropriate to the Technical service provider or RM Helpdesk 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 our 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.

Network management (user access, backup)

The Federation

- Uses individual, audited log-ins for all users - the London USO system;
- Uses guest accounts occasionally for external or short-term visitors for temporary access to appropriate services
- Ensures the Systems Administrator / network manager is up-to-date with RM services and policies / requires the Technical Support Provider to be up-to-date with RM services and policies;
- Storage of all data within the school will conform to the UK data protection requirements (GDPR compliant)
- Pupils and Staff using mobile technology, where storage of data is online, will conform to the EU data protection directive where storage is hosted within the EU.

To ensure the network is used safely, this Federation:

- Ensures staff read and sign that they have understood the Federation'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 Federation' management information system is controlled through a separate password for data security purposes;
- 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 minutes 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 mobile equipment with anti-virus / spyware before it is connected to the network;
- Makes clear that staff are responsible for ensuring that all 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;
- 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 IT Technician; equipment installed and checked by approved Suppliers / LA electrical engineers
- 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;
- Provides pupils and staff with access to content and resources through the approved Learning Platform which staff and pupils access using their username and password (their USO username and password);
- 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 our broadband network for our CCTV system and have had set-up by provided by approved partners;
- 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 Federation IT systems regularly with regard to health and safety and security.

Password policy

- This Federation 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 it;
- 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.
- All staff are required to change their passwords to the network systems every 3 months. This is enforced by our systems policy.
- We require staff to change their passwords into the MIS, Office 365 USO admin site

E-mail

This Federation

- Provides staff with an email account for their professional use, Office365, and makes clear personal email should be through a separate account;
- Provides *highly* restricted (Safe mail) / simulated environments for e-mail with Key Stage 1 pupils; Uses Office 365 service with students as this has email content control.
- Does not publish personal e-mail addresses of pupils or staff on the Federation website. We use anonymous or group e-mail addresses, for example info@schoolname.la.sch.uk / head@schoolname.la.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 Office 365-provided 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. Finally, and in support of these, Office 365 Web Screen2 filtering monitors and protects our Internet access to the World Wide Web.

Pupils:

- We use Purple Mash Mail with pupils which is locked down ensuring pupils can only email those within the Campus email system.
- Pupils are introduced to, and use email as part of the Computing scheme of work.
- Pupils are taught about the safety and 'netiquette' of using email both in school and at home i.e. they are taught:
    - Not to give out their email 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 about themselves or others in e-mail, 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 emails, but to keep them as evidence of bullying;
    - Not to arrange to meet anyone they meet through email without having discussed with an adult and taking a responsible adult with them;
    - That forwarding 'chain' email letters is not permitted.
    - Pupils sign the school Agreement Form to say they have read and understood the e-safety rules, including email and we explain how any inappropriate use will be dealt with.

Staff:

- Staff can only use the Federation's own Microsoft Office365 email system on the school system
- Staff only use Microsoft Office365 email systems for professional purposes
- Access in school to external personal email accounts may be blocked
- Never use email to transfer staff or pupil personal data. We use secure, LA / DfE approved systems. These include: S2S (for school to school transfer); Collect; USO-FX, *named LA system;*
- 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 Federation Agreement Form AUP 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.

Federation website, other social media platforms and blog

- The Federation E-safety Lead takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;
- Uploading of information is restricted to designated individuals at each campus;
- The Federation web site complies with the statutory DfE guidelines for publications;
- Most material is the Federation'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 points of contact on the website are the campus address, telephone number and we use general email contact addresses, e.g. info@schooladdress or admin@schooladdress. Home information or individual e-mail identities will not be published;
- Photographs published on the website, other social media platforms and blog 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 or blog;
- We do not use embedded geodata in respect of stored images
- We expect staff using' Federation approved blogs or wikis to password protect them and run from the Federation website.

Social networking

- Staff are instructed not to run social network spaces for pupils 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.
- The school's preferred system for social networking will be maintained in adherence with the communications policy.
- Federation staff will ensure that in private use:
  - No reference should be made in social media to students / pupils, parents / carers or Federation 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 campuses within the Federation or local authority
  - Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Video Conferencing

This Federation

- Only uses the Office 365. We don't have any active video conferencing services. However, staff can use Microsoft Teams for video calls.
- Only uses approved or checked webcam sites;

CCTV

- We have CCTV within the campuses as part of our site surveillance for staff and student safety. We will not reveal any recordings without permission except where disclosed to the Police as part of a criminal investigation.

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

Strategic and operational practices

Within this Federation:

- The Federation Executive Co-Headteachers are the Senior Information Risk Officers (SIRO).
- Staff are clear who are the key contact(s) for key school information (the Information Asset Owners) are. We have listed the information and information asset owners in a spreadsheet.
- 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 in SIMS,

  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 the stakeholders 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. /
- 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 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 secure area(s) on the network to store sensitive documents or photographs.
- We require staff to log-out of systems when leaving their computer, but also enforce lock-out after 10 minutes idle time.
- We use the DfE S2S site to securely transfer CTF pupil data files to other schools.
- We use Schools Admissions system (SAMS) to transfer admissions data. This is used in partnership with RBG and is secure.
- We also use Egress to send emails to RBG.
- We store any Protect and Restricted written material in lockable storage cabinets in a lockable storage area.
- 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 Federation (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

6. Equipment and Digital Content

Personal mobile phones and mobile devices

- Mobile phones brought into its schools are entirely at the staff member, student's & parents' or visitors own risk. The Federation accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school.
- At primary campuses pupil mobile phones which are brought into school must be turned off and handed in to the School Admin Office on arrival at school. They can be collected from the School Admin Office at the end of the day. Secondary aged students are permitted to keep their phones on them however they should be switched off as soon as they enter the campus. Students are not allowed to use them on school premises or on an educational visit unless directed to by a staff member. Staff members may use their phones during school break times. 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 Executive Co-Headteachers or Campus Leaders. Such authorised use is to be monitored and recorded. All mobile phone use is to be open to scrutiny and the Executive Co-Headteachers are to be able to withdraw or restrict authorisation for use at any time if it is to be deemed necessary.
- The Federation 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 pupils need to contact each other during the school day, they should do so only through the campus's 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 will not be used in any way during lessons or formal school time. They should be switched off or silent at all times.
- Mobile phones and personally-owned mobile devices brought into school sites are the responsibility of the device owner. The Federation accepts no responsibility for the loss, theft or damage of personally-owned mobile phones or mobile devices.
- Mobile phones and personally-owned devices are not permitted to be used in certain areas within the school site, e.g. changing rooms and toilets.
- 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.
- In the secondary phase, personal mobile phones will only be used during lessons with permission from the teacher.
- 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.

Students' use of personal devices

- The Federation accepts that there may be particular circumstances in which a parent wishes their child to have a mobile phone for their own safety.
- If a pupil needs to contact his or her parents or carers, they will be allowed to use a campus phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.
- Pupils should protect their phone numbers by only giving them to trusted friends and family members. Pupils will be instructed in safe and appropriate use of mobile phones and personally-owned devices and will be made aware of boundaries and consequences.

Staff use of personal devices

- Any permitted images or files taken in school must be downloaded from the device and deleted in school before the end of the day.
- 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 unless they have permission from the Executive Co-Headteachers for exceptional circumstances. E.g. safeguarding issue
- Staff will be issued with a Federation 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.

- Staff should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of students unless they have been given permission by the Executive Co-headteachers or Campus Leaders. Campus iPads are available for taking photographs and videos.
- 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, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes.

Digital images and video

Within this Federation:

- We gain parental / carer permission for use of digital photographs or video involving their child as part of the school agreement form when their child joins the Federation
- 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 Federation's Acceptable Use Agreement 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 Federation web site, in the prospectus or in other high-profile publications the Federation site will obtain individual parental or pupil permission for its long-term use
- Each campus blocks/filters 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 ICT 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 Federation-owned hardware will be recorded in a hardware inventory.
- Details of all Federation-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.

Appendix 1 - Pupil E-Safety Agreement KS1

I will check with an adult before using the internet. 	I will tell an adult if I see something I don't like on screen or if something makes me feel worried.
KI will only click on icons and links when I know they are safe. purple mash EducationCity 	I will keep my personal information, my name, address, my school, my pictures "Top Secret" and not share it on an app or a website.

My Name:

My Class:

Parent/Carer's Name:

Parent/Carer's Signature:

Date:

Parent/Carer

We understand that your child is too young to give informed consent on their own; however, we feel it is good practice to involve them as much as possible in the decision-making process, and believe a shared commitment is the most successful way to achieve this.

Please read the pupil agreement with your child, get them to write their name and sign to give permission on their behalf.

I have read and understand these rules and agree to them with my parent/carer's support.

My Name:

My Class:

Parent/Carer's Name:

Parent/Carer's Signature:

I have read and understood the e-safety agreement and give permission for my child to access the internet at school, and will encourage them to abide by these rules.

I have read and understand these rules and agree to them with my child

My Name:

My Class:

Parent/Carer's Name:

Parent/Carer's Signature:

All children will receive advice on e-safety at school.

Appendix 2 - Pupil E-Safety Agreement KS2

Pupils e-safety agreement

For my own personal safety – everywhere!

- I will ask permission from a member of staff before using the internet at school.
- I am aware of "stranger danger" when online and will not agree to meet online friends/stranger.
- I will tell an adult about anything online which makes me feel uncomfortable.
- I will not try to bypass the system to reach websites the school has blocked.
- I understand that the school may check my files and may monitor the web pages I visit.
- When in school I will only contact people with my teacher's permission.
- I will be very careful when sharing pictures or videos of myself or my friends.
- If I am in school, I will always check with a teacher.
- I will not put my "Personal Information" online. (My full name, birthday, phone number, address, postcode, school etc.)

To keep the system safe

- I will only use my own login and password, which I will keep secret.
- I will not access other people's files.
- I will not play games on a school computer unless my teacher has given me permission.
- I will not install software on school computers.
- I will not use the system for gaming, gambling, shopping, or uploading videos or music.

Responsibility to others

- The messages I send will be polite and responsible.
- I will not upload images or videos of other people without their permission.
- Where work is copyrighted (including music, videos and images,) I will not either download or share with others.
- I understand that the school may take action against me if I am involved in inappropriate behaviour on the internet and or on mobile devices.

Personal Devices

- The school cannot accept responsibility for loss or damage to personal devices.
- It is not permitted for pupils to use Mobile Phones during the school day.
- Phones should not be brought into school unless there is a genuine reason for doing so and my parents have approved this.
- If I have to bring my phone into school, I will hand it into my teacher at registration and get it back at the end of the school day.
- Other devices (e.g. Games consoles, cameras, wearable technology) should not be brought into school, unless my teacher has given me permission.

I have read and understand these rules and agree to them
My Name: My Signature: My Class: Date:

Koinonia Federation Primary Phases

Pupils e-safety contract- Woolwich, Peninsula, Christ Church Please complete, sign and return to the class teacher.	
Pupil:	Class:
Pupil Agreement I have read and I understand the pupils e-safety agreement, and will abide by the rules which are designed to keep both myself and the school safe	
Signed:	Date:
Parent/Carer Consent I have read and understood the e-safety agreement and give permission for my child to access the internet at school, and will encourage them to abide by these rules. I understand that the school will take reasonable precautions to ensure pupils cannot access inappropriate materials. I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's e-safety. I will ensure that any pictures taken during school events that include other children will not be shared using social media.	
Signed:	Date:
Please print name:	

Appendix 3 - Student E-Safety Agreement KS3/4

ACCEPTABLE USER PROCEDURES

At St Mary Magdalene School, we believe that expertise in the use of Information and Communication Technology will play an increasingly important role in the futures of our students. Computers offer access to a wide range of information to support study in all areas of the curriculum. Computers are provided and maintained for the benefit of all students and, therefore the School insists that students adhere to the rules set out below for the acceptable use of the equipment.

Computer Rules

- Students must not install or download programmes of any type on a machine, or store programmes on the computer or network drives without permission.
- Students must not damage, disable or otherwise harm the operation of, the computer or the network, or intentionally waste resources, including paper, ink, and toner cartridges.
- Students will not use the network for commercial purposes, e.g. buying or selling goods.
- Students must not disclose their password to others, or use the password intended for the use of another student.
- Students making use of the network must do so in a way that does not harass, harm, offend or insult others. Students are expected to respect and not attempt to bypass security in place on the computers or network. Accessing, copying, removing or otherwise altering other people's work or attempting to alter the settings of the computer are not acceptable and will result in sanctions being taken against the offender.
- Students should never have food or drink near their computers keeping computers clean and safe from any damage
- Teachers in the ICT suites have the right to see and block any inappropriate use of the internet and hand out consequences as per the behaviour policy through the use of specialist monitoring software in the classroom.
- Students will respect others work and property and will not access copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- If students are caught damaging equipment, the School reserves the right to seek remuneration.

Internet Rules

- Students may only access the Internet for study purposes or for authorised or supervised activities.
- Students must not use the Internet to obtain, download, send or print or otherwise transmit material which is unlawful, obscene or abusive.
- Students are expected to respect the work and ownership rights of other students, staff and persons outside of the school. This includes abiding by copyright laws.
- Students must not engage in social media over the Internet. Students are not permitted to access social networking sites for personal use. Though the school internet link or by using any of the school's ICT equipment. Should anyone unintentionally enter a social networking site he/she must exit site immediately. This could lead to consequences whereby the use of ICT maybe denied for a certain amount of time. In addition you must not give personal information such as addresses or telephone numbers to those they contact through electronic mail.

We have read and understood the E-Safety and I.C.T. Agreement

Parent's or carer's signature: ________________________________ Date: ___________________

Student's signature: ____ Date: ____________________

E-SAFETY AND ICT AGREEMENT

At St Mary Magdalene we take E-Safety very seriously and can understand the misuse of technology can lead to very serious consequences inside and outside of school. It is very important to read the statements below and understand if any of these are in breach then it can lead to consequences depending on the severity.

- Students Will be taught what Internet use is acceptable and what is not, and will be given clear objectives for internet use through their ICT/Computing lesson at the beginning of each academic year.
- Students are not permitted to use personal digital equipment, including mobile phones and cameras to record images of students or staff within the school environment, or when on educational visits. Unless pre-approved by a member of SLT.

Cyberbullying

Cyberbullying is bullying through the use of communication technology like a mobile phone, emails, text messages. This can take many forms for example

- Sending threatening or abusive text messages or emails, personally or anonymously
- Making insulting comment about someone on a website, social media, social networks (Snapchat, Instagram, Facebook etc)
- Making or sharing derogatory or embarrassing videos of someone via a mobile phone email.
- Abusive language or images used to bully, harass, threaten another whether spoken or written (through electronic means).

Within our school behaviour policy and acceptable user policy the use of web, text message social media sites, email, video or audio to bully another student or member of staff could lead to serious consequences and will not be tolerated.

As the parent or legal guardian of the student named below, I grant permission for them to have access to use the Internet and ICT facilities at school.

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school will take every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. These steps include using an educationally filtered service, restricted access email*, employing appropriate teaching practice and teaching e-safety skills to pupils.

I understand that the school can check my child's computer files, and the internet sites they visit, and that if they have concerns about their e-safety or e-behaviour that they will contact me.

I will support the school by promoting safe use of the internet and digital technology at home and will inform the school if I have any concerns over my child's e-safety.

We have read and understood the E-Safety and I.C.T. Agreement

Parent's or carer's signature: ____________________________ Date: _______________

Student's signature: __________________________________ Date: _______________

USE OF DIGITAL IMAGES

The use of multi-media is an integral part of the curriculum.

We need your permission before we can photograph or make recordings of your daughter/son.

We follow the following rules for any external use of digital images:

- We will not name the pupil in the image.
- Where showcasing examples of pupils work we only use their first names, rather than their full names.
- If showcasing digital video work to an external audience, we take care to ensure that pupils aren't referred to by name on the video, and that pupils' full names aren't given in credits at the end of the film. Only images of pupils in suitable dress are used. Staff are not allowed to store photographs or videos on their personal equipment.

Examples of how digital photography and video may be used include:

- Your child being photographed (by the classroom teacher, teaching assistant or another child) as part of a learning activity; e.g. photographing children at work and then sharing the pictures on the Interactive whiteboard in the classroom allowing the children to see their work and make improvements.
- Your child's image for presentation purposes around the school; e.g. in school wall displays and PowerPoint presentations to capture images around the school or in the local area as part of a project or lesson.
- Your child's image for presentation purposes; where only children and adults within the school community will be able to access and view, and will require a login and password to do so.
- Your child's image being used in a presentation about the school and its work in order to share its good practice and celebrate its achievements, which is shown to other parents, schools or educators and on the school website; e.g. within a CDROM / DVD or a document sharing good practice; in our school prospectus or on our school website. In rare events, your child's could appear in the media if a newspaper photographer or television film crew attend an event.

Note: If we, or you, wanted your child's image linked to their name we would contact you separately for permission, e.g. if your child won a national competition and wanted to be named in local or government literature.

Use of digital images - photography and video: I agree to the school using digital images and video of my child as described in the document 'Use of digital and video images' for school the school website and blog. I have read and understood this document. I understand that images will only be used to support learning activities or in publicity that reasonably promotes the work of the school, and for no other purpose.

We have read and understood the information above on the use of digital images

Parent's or carer's signature: ________________________________ Date: ________________

Student's signature: __________________________________ Date: ________________