Acceptable Use of Technology & E-Safety Policy

Introduction

ICT in the 21st Century is an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment. Within this, schools equally have a duty to ensure that this is done safely and to ensure that pupils are taught about the importance of staying safe online and the responsible use of technology.

This policy must be read in conjunction with our Federation safeguarding Policy

AIMS of the Policy

- **To establish the ground rules we have at the Federation for using any technology**
- **To describe how these fit into the wider context of other Federation policies that are relevant e.g. Safeguarding, Code of Conduct, Behaviour etc**
- **To demonstrate the methods used to protect children from sites containing any material that is deemed to be inappropriate or harmful because of content that is pornographic, sexually explicit, violent, extremist or radicalising, or discriminatory on the grounds of any of the 7 protected characteristics ion the Equality Act 2010.**

Information and Communications Technology covers a wide range of resources and it is important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Apps
- E-mail, Instant Messaging and chat rooms
- Social Media, including Facebook and Twitter
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices including tablets and gaming devices
- Online Games
- Learning Platforms and Virtual Learning Environments
- Blogs and Wikis
- Podcasting
- Video sharing
- Downloading
- On demand TV and video, movies and radio / Smart TVs

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks and responsibilities associated with the use of these Internet technologies. At **The Federation,** we understand the responsibility to educate our pupils on eSafety Issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using all forms of technology.

As a Federation we will record and monitor safety incidences as set out in the LSCB strategy and keep up to date with the emergence of new technologies. We will employ robust in-house management and communication strategies to ensure that issues that arise are tackled swiftly and appropriately. (See appendix A)

Technology Covered in this Policy

This policy (for all staff, governors, regular visitors [for regulated activities] and pupils) is inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, mobile devices, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones and other mobile devices)

Background

Definition of Safeguarding

Safeguarding children and protecting them from harm is everyone's responsibility. Everyone who comes into contact with children and families has a role to play. The following is the accepted definition of 'Safeguarding' and the promotion of wellbeing for children:

- protecting children from maltreatment;
- preventing impairment of children's health or development;
- ensuring that children grow up in circumstances consistent with the provision of safe and effective care; and
- taking action so as to enable children to have optimum life chances and enter adulthood successfully and have the best outcomes

Local authorities have overarching responsibility for safeguarding and promoting the welfare of all children and young people in their area. They have a number of statutory functions under the 1989 and 2004 Children Acts which make this clear, and this guidance sets these out in detail. This includes specific duties in relation to children in need and children suffering, or likely to suffer, significant harm, regardless of where they are found, under sections 17 and 47 of the Children Act 1989. Further information on this can be found in our Federation Safeguarding Policy

Definition of E-Safety

In addition to the definition set out in above, the term e-safety is specifically defined for the purposes of this document as the process of limiting the risks to children and young people when using Internet, Digital and Mobile Technology (IDMTs).

The Federation Vision

Our vision is that all children, parents/carers and all those working with children recognise these risks and potential dangers that may arise from the use of technology in all forms, that they understand how to mitigate these risks and are able to recognise, challenge and respond appropriately to any e-safety concerns so that children are kept safe

Potential Risks

We have a greater understanding of the extent of day to day dangers the virtual world can pose to children, including:

- being groomed online by adults with the ultimate aim of exploiting them sexually
- being bullied by others via social networking sites etc known as cyber bullying
- the taking of inappropriate / indecent images of children which are then uploaded and circulated via websites or networking sites. This is a criminal offence under s45 of the sexual offences act.

- the exposure of children to inappropriate / indecent / harmful images or material – including violence, sexual content (including pornography), content that is discriminatory on the grounds of race, gender, sex, religion, disability or sexual orientation.
- being exposed to the glorification and promotion of gang culture through gang websites, chat rooms, forums.
- the targeting of children by groups wishing to radicalise children online through content that appears on websites, chat forums or direct contact (e-mail / social media)

Ignoring these dangers would be a breach in our responsibilities in Working Together to Safeguard Children March 2015.

E-Safety Complaints

Please follow the Federation **Complaints Policy**

We make every effort to resolve low level issues internally, and these are recorded locally. All factors in relation to the complaint must be clearly established in order to have substance. Complaints about an employee's IDMT misuse should be escalated to the Heads of School immediately, and be managed according to our **Safeguarding Children Policy**. We have the ability to scrutinise IDMT use in particular, we have the ability to identify sites accessed. Potentially illegal issues must always be referred to the police in the first instance.

SECTION ONE – Keeping Children and Young People Safe

Education and Learning

The Federation provides internet access to children and we ensure that this is done in a way that is safe and age appropriate, by way of appropriate filtering systems. Our children agree to adhere to our e-safety rules and this policy. At present, the school endeavors to deny access to social networking and online games websites to pupils within school

Throughout the curriculum and in whole schools assemblies and class workshops, all pupils are taught about the risks and responsibilities as well as the educational rewards of using technology. Pupils are taught to:

- be cautious about the information given by others on such websites, for example users not being who they say they are.
- avoid placing images of themselves (or details within images that could give background details) on such websites and to consider the appropriateness of any images they do post.
- avoid giving out personal details on websites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, IM/ email address, specific hobbies/ interests)
- set and maintain their online profiles to maximum privacy and deny access to unknown individuals
- be wary about publishing specific and detailed private thoughts and information online
- report any incidents of Cyberbullying to the school
- be aware of the age restrictions on many social media applications (usually 13+)

Filtering

Levels of internet access and supervision must be appropriate and suitable for the children - however we recognise that there may be websites that staff may wish to access for research that might normally be filtered out e.g. google images. Access controls (filtering) fall into several categories:

- Blocking strategies to prevent access to unsuitable sites
- Walled garden of 'allow list' restricts access to a list of approved sites
- Dynamic filtering examines web pages or email for unsuitable words
- Rating systems give each web page a rating for sexual, profane, violent or other unacceptable content
- Access monitoring records the Internet sites visited by individual users.

Attempted access to an unsuitable site will result in a report.

At each Federation site we use a system approved by the LGfL. We make regular checks to ensure that filtering methods are age appropriate, effective and reasonable. Access to inappropriate material is reported to the Headteacher / Child Protection Lead or a Deputy who will escalate this to RM and the onsite technician.

If staff or pupils discover an unsuitable site, the screen must be switched off / closed and the incident reported immediately to the e-safety coordinator or teacher as appropriate.

Illegal Downloading

Children are made aware that if they attempt to download copyright protected files they are breaking the law or infringing intellectual property rights. Our Federation ICT network at does not permit any child to download anything.

Cyber-Bullying

Cyber bullying is defined as the act of using the Internet, mobile phones, video games, or other technology gadgets to send, text, or post images or other material intended to hurt or embarrass another person. "It is also defined as acts of aggression through computers, mobile phones, and other electronic devices" (Jackson & Cohen, 2012)

At The Federation we have a **zero tolerance policy on this kind of behaviour**. The law gives schools the power to intervene in such cases even when they have happened outside of school time, using technology that is not the schools. (Please see Behaviour policy and Dfe Guidance from Sept 2012)

Those who participate in online bullying often use groups of friends to target their victims. An action as innocent as adding derogatory comments to another's photograph could rapidly spiral out of control and young people may not realise that their actions constitute bullying. The following are the most commonly reported types of cyberbullying:

- Email – Can be sent directly to an individual or group to encourage them to participate in the bullying and can include derogatory comments or harassment.
- Instant messaging – messages can be sent directly to an individual or group who can then be included in the conversation. See above
- Social networking sites – anonymous profiles can be set up to make fun of someone and each person contributing to these pages can soon worsen the problem.
- Inappropriate and threatening comments and images can also be posted and circulated without consent.
- Mobile Phones – Anonymous and abusive text or video messages and photo messages and phone calls can be shared via phones. This includes the videoing and sharing of physical or sexual attacks (a criminal offence) on individuals.
- Interactive gaming – Games consoles allow users to chat online with anyone.
- Abuse of other online game players and the use threats.

- Hacking into the account of another user for malicious reasons
- Sending viruses – These can be sent from one person to another in order to destroy computers or delete personal information from their hard drive.
- Abusing personal information – Personal / sensitive information (including videos and photographs) being uploaded onto the internet without the victim's permission.

Some instances of cyberbullying do escalate into physical bullying. We take all instances of cyberbullying extremely seriously and we record all instances that are reported to us. We will escalate concerns to the police where necessary. We encourage children to store the electronic records of abuse which will be essential in any subsequent investigation.

Monitoring E-Safety Incidences and Reporting Abuse

Any form of electronic or digital abuse (as defined in our child protection policy) will be reported to CEOP service www.ceop.police.uk and also to the Headteacher (Child protection lead). Any incidences which place a young person in immediate danger will reported to 999.

We recommend that the CEOP 'Report Abuse' tool is downloaded onto all computer browsers. This allows instant online access to report any form of online abuse. We encourage our older children to download this tool directly onto their electronic devices.

We monitor e-Safety incidences which is crucial for establishing any patterns and learning lessons quickly (see Appendix A): It is recommended by the Southwark children's safeguarding board that we record the following:

- A description of the e-safety incident
- Who was involved
- How the incident was identified
- What actions were taken and by whom
- Conclusion of the incident
- Lessons learnt – to inform ongoing policy and practice

Children Sending E-mails

All children use a class/ group e-mail address (dependant on year group). The forwarding of chain emails is not permitted in school. All pupils in school know to alert the class teacher if any chain emails causing them anxiety. All pupil e-mail users are expected to adhere to the rules of responsible online behaviour, particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission, virus checking and the opening of attachments from unknown sources. Pupils must immediately tell a teacher/ trusted adult if they receive an offensive or upsetting e-mail. Pupils are introduced to e-mail as part of the Computing Programme of Study and they may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes. All pupils are reminded that school based email and internet activity can be monitored and explored further if required.

Pupils and Mobile Phones

Pupils are allowed to bring personal mobile devices/phones to school but must not use them for personal purposes within lesson time. At all times the device must be switched off and handed into the school office. The school is not responsible for the loss, damage or theft of any personal mobile Device. Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

Pupils with Additional Needs

The school endeavours to create a consistent message with parents/carers for all pupils and this in turn should aid establishment and future development of the schools' eSafety rules. However, staff are aware that some pupils may require additional support or teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of eSafety issues. Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of eSafety. Internet activities are planned and well managed for these children and young people

Involving Parents and Carers

We believe that it is essential for parents/carers to be fully involved with promoting eSafety both in and outside of school and to be aware of their responsibilities. We regularly consult and discuss eSafety with parents/ carers and seek to promote a wide understanding of the benefits of new technologies, together with the associated risks. Parents/carers are invited to regular eSafety talks in school and are asked to read through and sign acceptable use agreements on behalf of their child on admission to the school.

Parents/carers are required to make a decision as to whether they consent to images of their child being taken and used in the public domain (eg, on school website) Parents/carers are expected to sign a Home School agreement. The school disseminates information to parents relating to eSafety where appropriate in the form of Information evenings, posters, website information and newsletter items.

SECTION TWO – Keeping Adults Safe

As well as a duty to keep children safe, The Federation also takes seriously its duty to protect adults with regard to the use of technology in the workplace. As such we ask that all adults read and sign a copy of the Internet Safety and Acceptable Use Policy for Staff, Governors & Authorised visitors (Annex C).

Monitoring

Authorised ICT staff may inspect any ICT equipment owned or leased by the school at anytime without prior notice. ICT authorised staff may monitor, intercept, access, inspect, record and disclose telephone calls, e-mails, instant messaging, internet/intranet use and any other electronic communications (data, voice, video or image) involving its employees or contractors, without consent, to the extent permitted by law. This may be to confirm or obtain school business related information; to confirm or investigate compliance with school policies, standards and procedures; to ensure the effective operation of school ICT; for quality control or training purposes; to comply with a Subject Access Request under the Data Protection Act 1998, or to prevent or detect crime.

ICT authorised staff may, without prior notice, access the e-mail or voice-mail account where applicable, of someone who is absent in order to deal with any business-related issues retained on that account.

All monitoring, surveillance or investigative activities are conducted by ICT authorised staff and comply with the Data Protection Act 1998, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000.

Please note that personal communications using School ICT may be unavoidably included in any business communications.

Personal Data

The Federation holds personal data on learners, staff and others 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 potentially damage the reputation of the school. Everybody in the school community 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.

Breaches

A breach or suspected breach of policy by a school employee, contractor or pupil may result in the temporary or permanent withdrawal of school ICT hardware, software or services from the individual concerned.

For staff any policy breach is grounds for disciplinary action in accordance with the school Disciplinary Procedure or, for Support Staff, in their Probationary Period as stated. Policy breaches may also lead to criminal or civil proceedings.

The Information Commissioner's powers to issue monetary penalties came into force on 6 April 2010, allowing the Information Commissioner's office to serve notices requiring organisations to pay up to £500,000 for serious breaches of the Data Protection Act.

The data protection powers of the Information Commissioner's Office are to:

- Conduct assessments to check organisations are complying with the Act;
- Serve information notices requiring organisations to provide the Information Commissioner's Office with specified information within a certain time period;
- Serve enforcement notices and 'stop now' orders where there has been a breach of the Act, requiring organisations to take (or refrain from taking) specified steps in order to ensure they comply with the law;
- Prosecute those who commit criminal offences under the Act;
- Conduct audits to assess whether organisations' processing of personal data follows good practice,
- Report to Parliament on data protection issues of concern
- For pupils, reference will be made to the school's behaviour policy also.

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's relevant responsible person. Additionally, all security breaches, lost/stolen equipment or data (including remote access SecureID tokens and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the relevant responsible person. The relevant responsible individuals in the school are The Headteacher, The child protection officer or a member of SLT.

Staff Sending Emails

The use of e-mail within most schools is an essential means of communication for both staff and pupils. For this reason it is important that all staff check their email regularly. In the context of school, e-mail should not be considered private. Educationally, e-mail can offer significant benefits and we recognise that pupils need to understand how to use e-mail in relation to their age and how to behave responsible online.

Managing Email

The school gives all staff & governors their own e-mail account to use for all school business. This is to protect staff, minimise the risk of receiving unsolicited or malicious e-mails and avoids the risk of personal information being revealed. Staff & governors should use their school email for all professional communication. It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary e-mail histories can be traced. Staff should not contact pupils, parents or conduct any school business using personal e-mail addresses.

The school requires a standard disclaimer to be attached to all e-mail correspondence, stating that, 'the views expressed are not necessarily those of the school or the LA'.

Staff must inform the Headteacher or Deputy on their site if they receive an offensive e-mail. Any emails created or received as part of your school job will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000. You must therefore actively manage your e-mail account as follows:

- Organise e-mail into folders and regularly delete old / unwanted mail.
- e-mails containing personal, confidential, classified or financially sensitive data sent to external third parties or agencies should be marked as confidential (refer to the Section 'E-Mailing personal, sensitive confidential or classified information')
- Use only your own school e-mail account (not that of other staff members)
- Do not send / forward attachments internally unnecessarily.
- Do not use school e-mail for personal business
- Never open attachments from untrusted sources; consult your network manager first
- Be aware that school based email and internet activity can be monitored and explored further if required

Emailing Personal, Sensitive or Confidential / Classified Information.

Where e-mail must be used to transmit such data:

- Obtain consent from your manager to provide the information by e-mail
- Verify the details, including accurate e-mail address, of any intended recipient.
- Verify (by phoning) the details of a requestor before responding to e-mail requestsfor information
- Do not copy or forward the e-mail to any more recipients than is absolutely necessary
- Do not send the information to any person whose details you have been unable to verify (usually by phone)
- Send the information as an encrypted document **attached** to an e-mail
- Provide the encryption key or password by a **separate** contact with the recipient(s)
- Do not identify such information in the subject line of any e-mail
- Request confirmation of safe receipt

Personal Mobile Devices (including phones)

Staff are permitted to bring in personal mobile phones and devices for their own use. Under no circumstances should a member of staff contact a pupil or parent/ carer using their personal device use it or to take video footage or still images of pupils or any other school activity. Staff must ensure that they are aware of and adhere to the zones in which the use of personal mobile phones is permitted (Staff room and office spaces). Mobile phones are not allowed to be used by staff in classrooms. The sending of inappropriate text messages between any member of the school community is not allowed.

The school is not responsible for the loss, damage or theft of any personal mobile Device. Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

School Provided Mobile Devices (including phones)

Devices provided by the school must only be used for school business and are subject to the same rules when being used offsite. Permission must be sought before any image or sound recordings are made on the devices of any member of the school community. Where the school provides mobile technologies such as phones, laptops and iPads for offsite visits and trips, only these devices should be used.

Use of Social Media

Facebook, Twitter and other forms of social media are increasingly becoming an important part of our daily lives. The Federation uses the school website to communicate with parents and carers. At present the Federation does not have an official social media presence and the main Federation website if our official platform for online presence. In relation to social media, the following applies:

- Staff ***are not*** permitted to access their personal social media accounts using school equipment at **any time/ when they are 'in loco parentis' (usually from 8:45 – 3:30)**
- Staff are able to setup Social Learning Platform accounts, using their school email address, in order to be able to teach pupils the safe and responsible use of Social Media
- Staff, governors, pupils, parents and carers are regularly provided with information on how to use social media responsibly and what to do if they are aware of inappropriate use by others
- Staff, governors, pupils, parents and carers are aware that the information, comments, images and video they post online can be viewed by others and copied.
- Staff, governors, pupils, parents and carers are aware that their online behaviour should at all times be compatible with UK law

Use of Land Line Telephones

School telephones are provided specifically for school business purposes. Personal usage is a privilege that will be withdrawn if abused. Staff may make or receive personal telephone calls provided:

- They are infrequent, kept as brief as possible and do not cause annoyance to others
- They are not for profit or to premium rate services
- They conform to this and other relevant HCC and school policies.

Be aware that the laws of slander apply to telephone calls. Whilst a telephone call may seem to have a temporary and private existence it still qualifies as admissible evidence in slander law cases. Ensure that your incoming / outgoing telephone calls do not interfere with your duties within school and primarily learning and teaching. Any telephone calls during teaching time should be in the event of an emergency only. Follow the appropriate procedures (Emergency Contingency Plan) in the event of receiving a telephone call containing a bomb threat. These procedures should be made readily available throughout your office. If you do not have a copy, please ask download one from the Shared Drive (under Federation Policies / H&S Policies / Emergency contingency plans).

Section Three - Keeping Data and Equipment Protected

Computer Viruses

- All files downloaded from the Internet, received via e-mail or on removable media such as a memory stick must be checked for any viruses using school provided anti-virus software before being used.
- Never interfere with any anti-virus software installed on school ICT equipment.
- If your machine is not routinely connected to the school network, you must make provision for regular virus updates through your IT team.
- If you suspect there may be a virus on any school ICT equipment, stop using the equipment and contact your ICT support provider immediately. The ICT support provider will advise you what actions to take and be responsible for advising others that need to know.

Data Security

The accessing and appropriate use of school data is something that the school takes very seriously. The school gives relevant staff access to its Management Information System, with a unique username and password and it is the responsibility of everyone to keep passwords secure. All staff are aware of their responsibility when accessing school data and have been issued with the relevant guidance documents and the Policy for ICT Acceptable Use

All staff should:

- keep all school related data secure. This includes all personal, sensitive,confidential or classified data
- avoid leaving any portable or mobile ICT equipment or removable storage media in unattended vehicles. Where this is not possible, keep it locked and out of sight
- be responsible to ensure the security of any personal, sensitive, confidential and classified information contained in documents faxed, copied, scanned or printed. This is particularly important when shared mopiers (multi-function print, fax, scan and copiers) are used
- notify the recipient before sensitive / confidential faxes are sent.
- read the Southwark Council – Information and IT security Policies April 2013

Protecting Personal, Sensitive, Confidential and Classified Information.

All staff agree to:

- Ensure that any school information accessed from your own PC or removable media equipment is kept secure, and remove any portable media from computers when not attended.
- Ensure you lock your screen before moving away from your computer during your normal working day to prevent unauthorised access
- Ensure the accuracy of any personal, sensitive, confidential and classified information you disclose or share with others
- Ensure that personal, sensitive, confidential or classified information is not disclosed to any unauthorised person
- Only download personal data from systems if expressly authorised to do so by your manager
- Not post on the internet personal, sensitive, confidential, or classified information, or disseminate such information in any way that may compromise its intended restricted audience

- Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information
- Ensure hard copies of data are securely stored and disposed of after use in accordance with the document labelling.

Protective Marking of Official Information

Staff must be trained to understand that they are personally responsible for securely handling any information that is entrusted to them, in line with local business processes. The following general guidance applies:

- There is no requirement to mark routine OFFICIAL information.
- Optional descriptors can be used to distinguish specific type of information.
- Use of descriptors is at an organisation's discretion.
- Existing information does not need to be remarked.
- In such cases where there is a clear and justifiable requirement to reinforce the 'need to know', assets should be conspicuously marked: '**OFFICIAL–SENSITIVE'**

Passwords and Passwords Security

- **Always use your own** personal passwords
- Make sure you enter your personal passwords each time you logon. Do not include
- passwords in any automated logon procedures
- Staff should change temporary passwords at first logon
- Change passwords whenever there is any indication of possible system or password compromise
- Do not record passwords or encryption keys on paper or in an unprotected file
- **Only disclose your personal password to authorised ICT support staff when necessary, and never to anyone else**. Ensure that all personal passwords that have been disclosed are changed once the requirement is finished
- **Never tell a child or colleague your password**

Relevant Responsible Person

Senior members of staff should be familiar with information risks and the school's response. The senior leadership team (Headteachers and Deputies) have the following responsibilities:

- to lead on the information risk policy and risk assessment
- to advise school staff on appropriate use of school technology
- to act as an advocate for information risk management

The Office of Public Sector Information has produced *Managing Information Risk*, [http://www.nationalarchives.gov.uk/services/publications/information-risk.pdf] to support relevant responsible staff members in their role.

Information Asset Manager

For information such as assessment records, medical information and special educational needs data, a responsible member of staff should be able to identify across the school:

- what information is held, and for what purposes
- what information needs to be protected, how information will be amended or added to over time
- who has access to the data and why
- how information is retained and disposed of

As a result this manager is able to manage and address risks to the information and make sure that information handling complies with legal requirements. However, it should be clear to all staff that the handling of secured data is everyone's responsibility – whether they are an employee, consultant, software provider or managed service provider. Failing to apply appropriate controls to secure data could amount to gross misconduct or even legal action.

Disposal of Redundant ICT Equipment

All redundant ICT equipment will be disposed of through an authorised agency. This should include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data. All redundant ICT equipment that may have held personal data will have the storage media over written multiple times to ensure the data is irretrievably destroyed, or if the storage media has failed it will be physically destroyed. We will only use authorised companies who will supply a written guarantee that this will happen and will ensure that hard drives from machines no longer in service are removed and stored securely or wiped clean. We will securely dispose of removable media that may hold personal data.
It is essential that any hard drives which may have held personal or confidential data are 'scrubbed' in way that means the data can no longer be read. It is not sufficient to simply delete the files or reformat the hard drive. Whoever you appoint to dispose of the equipment must provide a **written guarantee** that they will irretrievably destroy the data by multiple over writing the data.

Disposal of any ICT equipment will conform to:

The Waste Electrical and Electronic Equipment Regulations 2006
The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007
Data Protection Act 1998
Electricity at Work Regulations 1989

The school will maintain a comprehensive inventory of all its ICT equipment including a record of disposal which will include:

- Date item disposed of
- Authorisation for disposal, including:
    - verification of software licensing
    - any personal data likely to be held on the storage media? *
- How it was disposed of eg waste, gift, sale
- Name of person & / or organisation who received the disposed item
- Any redundant ICT equipment being considered for sale / gift will have been subject to a recent electrical safety check and hold a valid PAT certificate

ZOMBIE ACCOUNTS

Zombie accounts refers to accounts belonging to users who have left the school and therefore no longer have authorised access to the school's systems. Such Zombie accounts when left active can cause a security threat by allowing unauthorised access. The school ICT Technician will ensure that all user accounts are disabled once the member of the school has left. Prompt action on disabling accounts will prevent unauthorised access

SERVERS

- Always keep servers in a locked and secure environment
- Limit access rights
- Always password protect and lock the server
- Existing servers should have security software installed appropriate to the machine's specification
- Backup tapes should be encrypted by appropriate software
- Data must be backed up regularly
- Backup tapes/discs must be securely stored in a fireproof container
- Back up media stored off-site must be secure
- Remote backups should be automatically securely encrypted.

Review Procedure

There will be on-going opportunities for staff to discuss with the eSafety coordinator any eSafety issue that concerns them. This policy will be reviewed every (24) months and consideration will be given to theimplications for future whole school development planning The policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way

Further help and support

The Information Commissioner's Office https://ico.org.uk/
School's toolkit is available - Record Management Society website – http://www.rms-gb.org.uk/resources/848
Test your online safety skills http://www.getsafeonline.org
Data Protection Team – Email – accessinfo@southwark.gov.uk 0207 525 7511
Information Commissioner's Office – www.ico.org.uk
For additional help, email school.ictsupport@education.gsi.gov.uk

Current Legislation

Acts Relating to Monitoring of Staff email:

- Data Protection Act 1998
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Regulation of Investigatory Powers Act 2000
- Human Rights Act 1998

Other Acts Relating to eSafety:

- Racial and Religious Hatred Act 2006
- Sexual Offences Act 2003
- Communications Act 2003 (section 127)
- The Computer Misuse Act 1990 (sections 1 – 3)
- Malicious Communications Act 1988 (section 1)
- Copyright, Design and Patents Act 1988
- Public Order Act 1986 (sections 17 – 29)
- Protection of Children Act 1978 (Section 1)
- Obscene Publications Act 1959 and 1964
- Protection from Harassment Act 1997
- Acts Relating to the Protection of Personal Data
- Data Protection Act 1998
- The Freedom of Information Act 2000

Appendix A

E-Safety Concern and Record of Action

This form is to be used to record any incidences of cyberbullying or inappropriate use of technology that comes to our attention both in and out of school time.

Name of Victim	Year group/class	Site	Date
Type of technology that has been misused		Where is the technology located?	
Incident description			
Full names of all those involved (including year groups and sites)			
How do we know about the incident – who brought it to our attention?			
What actions were taken and by whom?			
Conclusion of the incident and lessons learnt – how was it dealt with and what will we do differently next time? (To be completed by E-Safety Lead / SLT)			
Report Completed by: Sign: Name:	Seen by Head teacher	Deputy	FSO

Appendix B

>>>Insert School logo and details>>>>

Dear Parent/ Carer

ICT including the internet, e-mail and mobile technologies has become an important part of learning in our school. We expect all children to be safe and responsible when using any ICT.

Please read and discuss these eSafety rules with your child and return the slip at the bottom of this page. If you have any concerns or would like some explanation please contact the Headteacher.

Please take care to ensure that appropriate systems are in place at home to protect and support your child/ren. We will support the school approach to on-line safety and not deliberately upload or add any text, image, sound or videos that could upset or offend any member of the school community or bring the school name into disrepute.

Parent/ carer signature

We have discussed this document with …….... (child's name) and we agree to follow the eSafety rules and to support the safe use of ICT at The Federation.

Parent/ Carer Signature ……..……..…….

Class …….. Date ……

Primary Pupil Acceptable Use Agreement / eSafety Rules

As a pupil at The Mayflower Federation I agree that:

I will only use ICT in school for school purposes

I will only use my class e-mail address or my own school e-mail address when emailing

I will only open e-mail attachments from people I know, or who my teacher has approved

I will not tell other people my ICT passwords

I will only open/delete my own files

I will make sure that all ICT contact with other children and adults is responsible, polite and sensible

I will not deliberately look for, save or send anything that could be unpleasant or nasty.

If I accidentally find anything like this I will tell my teacher immediately

I will not give out my own/others details such as name, phone number or home address.

I will not arrange to meet someone or send my image unless this is part of a school project approved by my teacher and a responsible adult comes with me

I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe

I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community

I know that my use of ICT can be checked and my parent/carer contacted if a member of school staff is concerned about my safety

I will not sign up for any online service unless this is an agreed part of a school project approved by my teacher

I will not use school technology for the purposes of private gaming (downloading or playing).

I understand that if this happens I will have my rights to Federation technology access withdrawn.

Signed……

Print Name……..

Annex C

Internet Safety and Acceptable Use Policy
for
Staff, Governors & Authorised visitors

In line with our policy on e-safety it is requested that all those using technology within any Federation site, read and sign the agreement below:

Internet Use

- Children and non-staff adults are not to use the Internet without staff supervision.
- Any web pages to be used for teaching purposes should be screened by a member of staff before use with children.
- Fire walls, content screening software or service providers with filtering facilities are to be used wherever possible.
- Children and non-staff adults are instructed in the responsible use of the Internet and are asked to report any unsuitable material directly to the ICT Manager or a member of the Senior Leadership Team promptly.
- Unsuitable content which is not blocked via the school filtering system should be reported to the Technology Faculty Leader.
- The internet should be used for curriculum, professional and administration purposes only.
- Personal use of Internet by staff is permitted outside of core teaching time.
- Staff must ensure that the internet for personal use that websites are closed down appropriately and machines logged off.
- Internet used out of school hours by children should always be under staff supervision.
- No information which could lead to the unauthorised identification or contact of an individual child or adult by a member of the public may be published on the Internet.
- Photographs of children may only be published on the Federation website by the website manager (with parental permission) but the children should **never** be named.
- Private contact details of staff or children (other than the School's contact details) must not be published on the Internet.
- The use of, or viewing of online gambling sites are strictly forbidden

E-mail Use

- Excessive unsolicited emails i.e. 'spam' to be reported to a technology team member. Under no circumstances should any accompanying attachments be opened.
- Any school business should only be conducted via the school email system provided.
- Use of personal email accounts to conduct school business is **not** permitted and school email accounts should **not** be used for personal uses.
- Personal e-mail accounts may be accessed by staff outside of core teaching time (subject to school filtering systems).
- All personal email accounts must be closed down appropriately when not in active use. Staff are requested to exercise extreme caution in accessing personal information via school ICT equipment or in school hours. Failure to do so may place children at risk of seeing or accessing unsuitable content which would be taken very seriously and may result in disciplinary procedures taking place.

- Personal use of e-mail addresses of children is not permitted.
- Personal use of e-mail by visitors and those outside of those outside the federation is not permitted, unless authorised by a staff member.
- No information which could lead to the unauthorised identification or contact of an individual child or adult by a member of the public may be emailed.
- Photographs of children may be emailed via school e-mail within the organisation freely, but if they are e-mailed outside the organisation parental permission will be needed. Names should not be included in external e-mails.

Responsible use of ICT facilities

- Staff and guests should be instructed in the responsible use of the ICT facilities.
- Staff and guests must not interfere with the work of others on the system either directly or indirectly.
- Staff must be aware that school based email and internet activity is monitored and explored further if required
- The facilities must be used in a responsible manner, in particular, staff and guests must not deliberately view, create or transmit material that is deemed / likely to be deemed as:
    - Obscene, defamatory or indecent
    - cause annoyance, inconvenience, anxiety or offence.
    - infringes the copyright of another person.
    - Introducing or causing viruses on Federation computer systems or networks.

If staff, students or guests are found to have infringed these guidelines, then the incident must be reported to the Head Teacher as soon as possible and depending upon the severity of the incident, a verbal or written warning may be given; the user may be allowed only restricted access to facilities; the user may lose the privilege of using the facilities; or the initiation of staff disciplinary procedures may result, or, in extreme cases, the police may be contacted.

Use and storage of Digital Images and Media

- Photographs and video taken of children should always be done using school equipment, never using personal cameras or mobile phones owned by members of staff or any other individuals in school.
- When pictures are stored on the network, they should be deleted once used and should never be stored beyond their purpose. Exceptions to this would be for school purposes such as the school brochure, or photographs used for publication purposes.
- Images of children at school should never be stored on home computers.
- School cameras which hold images of children should not be taken outside of the school unless on school business.

I agree to the terms set out in this agreement.
I understand that Internet use and e-mail use may be monitored.

Name: _____

Date: _____