ST MARY'S CATHOLIC PRIMARY SCHOOL

ACCEPTABLE USE OF ICT & MOBILE PHONES POLICY

DATE: - **13th November 2018**

CHAIR OF FINANCE COMMITTEE: - **……**

MINUTED: - **……**

DATE OF NEXT REVIEW: - **Autumn 2020**

REVIEW FREQUENCY:- **Bi-Annually**

St. Mary's Catholic Primary School

Acceptable Use of IT and Mobile Phones Policy

1 PURPOSE

The policy defines and describes the acceptable use of IT (Information and Communications Technology) and mobile phones for school-based employees. Its purpose is to minimise the risk to pupils of inappropriate contact from staff, to protect employees and schools from litigation and to minimise the risk to IT systems.

2 SCOPE

2.1 This policy deals with the use of IT facilities in school and applies to all school-based employees and other authorised users, e.g. volunteers.

2.2. Non school –based staff are subject to the County Council's IT Acceptable Use Policy.

3 SCHOOL RESPONSIBILITIES

3.1 The Governing Body is responsible for ensuring that its employees act in a lawful manner, making appropriate use of school technologies for approved purposes only.

3.2 The Governing Body is responsible for adopting relevant policies and the Headteacher for ensuring that staff are aware of their contents.

3.3 The School Business Manager is responsible for maintaining an inventory of IT equipment and a list of school laptops and other devices and to whom they have been issued.

3.4 If the Headteacher has reason to believe that any IT equipment has been misused they will always ensure that the procedures outlined in Suffolk Safeguarding Children Board Protocol: Allegations Against Persons who Work with Children and Part 4 of 'Keeping Children Safe in Education', DfE (2018) are adhered to and will seek appropriate advice from the Local Authority Designated Officer (LADO). The Suffolk LADO Service can be contacted on 0300-123-2044 or LADOCentral@suffolk.gcsx.gov.uk

3.5 The Headteacher should make it clear that internal school staff should not carry out any investigations unless they are both qualified and authorised to do so.

4 USER RESPONSIBILITIES

4.1 Staff found to be in breach of this policy may be disciplined in accordance with the disciplinary procedure. In certain circumstances, breach of this policy may be considered gross misconduct resulting in termination of employment. Users must report all suspected breaches of this policy to the Headteacher.

4.2 Users and their managers are responsible for ensuring that adequate induction, training and support is undertaken to implement this policy.

4.3 By logging on to IT systems, users agree to abide by this Acceptable Use policy and other policies that relate to the use of IT.

4.4 All users are expected to act in a responsible, ethical and lawful manner with the understanding that school electronic and manual information may be accessible to the public under the Freedom of Information Act 2000. Users should uphold privacy and confidentiality in accordance with the Data Protection Act 2018. Care must also be taken not to breach another person's copyright, trademark or design, nor to publish any defamatory content.

4.5 Staff who have been given the use of a school laptop, iPad or other device will be expected to sign for its use on receipt. Staff may use school equipment for authorised business use only, except as allowed for in paragraph 5.1.

4.6 Staff must follow authorised procedures when relocating IT equipment or taking mobile devices offsite.

4.7 No one may use IT resources in violation of license agreements, copyrights, contracts or national laws, or the Standing Orders, policies, rules or regulations of the school or the County Council.

4.8 Users are required to protect their password and not share their account details with others for their use, nor utilise another users' account or misrepresent their identity for any reason. Users must not under any circumstances reveal their password to anyone else.

4.9 No user shall access (e.g., read, write, modify, delete, copy, move) another user's personal electronic documents (including email) without the owner's permission or as allowed by this policy or by law.

4.10 Users must not load or download software on any device without the authorisation of the Headteacher. Periodic audits of software held on IT equipment will be undertaken.

4.11 Users must take care to store sensitive information, e.g. pupil data safely and to keep it password protected, on all school systems, including laptops and encrypted memory sticks.

4.12 Network connected devices must have school approved anti-virus software installed and activated. Users may not turn off anti-virus software. All users of IT resources have the responsibility to take precautions to prevent the initial occurrence and subsequent spreading of a computer virus. No one may knowingly create, install, run, or distribute any malicious code (e.g. viruses, Trojans, worms) or another destructive program on any IT resource.

4.13 No one may knowingly or willingly interfere with the security mechanisms or integrity of IT resources. No one may use IT resources to attempt unauthorised use, or interfere with the legitimate use by authorised users, of other computers on internal or external networks. Access to networks will be monitored.

4.14 Within the terms of the Data Protection Act 2018, Human Rights Act 1998 and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, the Academy Trust or school may record or inspect any information

transmitted through or stored in its computers, including e-mail communications and individual login sessions, without notice when:

- There is reasonable cause to believe the user has violated or is violating this policy, any guidelines or procedures established to implement this policy.
- An account appears to be engaged in unusual or unusually excessive activity.
- It is necessary to do so to protect the integrity, security, or functionality of IT resources or to protect the Academy Trust from liability.
- Establishing the existence of facts relevant to the business.
- Ascertaining or demonstrating standards which ought to be achieved by those using the IT facilities
- Preventing or detecting crime
- Investigating or detecting unauthorised use of IT facilities
- Ensuring effective operation of IT facilities
- Determining if communications are relevant to the business (for example, in the last resort where an employee is off sick or on holiday and business continuity is threatened)
- It is otherwise permitted or required by law.

4.15.1 Do not send private, sensitive or confidential information by unencrypted email – particularly to an external recipient - if accidental disclosure could lead to significant harm or embarrassment. The use of the Egress confidential email system should be used when appropriate. Anonymise personal data where possible e.g. by using initials. Use passwords on sensitive documents that must be sent to external recipients.

4.16 Websites should not be created on school equipment without the written permission of the Headteacher.

4.16.1 No one may use IT resources to transmit abusive, threatening, or harassing material, chain letters, spam, or communications prohibited by law. No one may abuse the policies of any newsgroups, mailing lists, and other public forums through which they participate from a school account.

4.17 The following content should not be created or accessed on IT equipment at any time:

- Pornography and “top-shelf” adult content
- Material that gratuitously displays images of violence, injury or death
- Material that is likely to lead to the harassment of others
- Material that promotes intolerance and discrimination on grounds of race, sex, disability, sexual orientation, religion or age
- Material relating to criminal activity, for example buying and selling illegal drugs
- Material relating to any other unlawful activity e.g. breach of copyright
- Material that may generate security risks and encourage computer misuse

4.18 It is possible to access or be directed to unacceptable Internet sites by accident. These can be embarrassing and such sites can be difficult to get out of. If staff have accessed unacceptable content or are in receipt of unacceptable material via email, they should inform the Headteacher. This may avoid problems later should monitoring systems be alerted to the content.

PERSONAL USE & PRIVACY

5.1 In the course of normal operations, IT resources are to be used for business purposes only. The school permits limited personal use of IT facilities by authorised users subject to the following limitations:

- Personal use must be in the user's own time and must not impact upon work efficiency or costs.
- The level of use must be reasonable and not detrimental to the main purpose for which the facilities are provided.
- Personal use must not be of a commercial or profit-making nature.
- Personal use must not be of a nature that competes with the business of the school or conflicts with an employee's obligations.

5.2 Personal use of the Internet must not involve attempting to access the categories of content described in section 4.18 that is normally automatically blocked by web filtering software.

6 MOBILE PHONE COMMUNICATION AND INSTANT MESSAGING

6.1 Staff are advised not to give their home telephone number or their mobile phone number to pupils. Mobile phone communication should be used sparingly and only when deemed necessary.

6.2 Photographs and videos of pupils should not be taken with mobile phones.

6.3 Staff are advised not to make use of pupils' mobile phone numbers either to make or receive phone calls or to send to or receive from pupils text messages other than for approved school business.

6.4 Staff should only communicate electronically with pupils from school accounts on approved school business, e.g. coursework.

6.5 Staff should not enter into instant messaging or social media communications with pupils.

7 Acceptable Use Agreement to be signed by new all school staff and volunteers and when any updates or amendments take place.

To be reviewed bi-annually.

Adoption/Review	Committee	Lead Person	Review Date
September 2016	WGB	J Sandvig	Autumn 2018
October 2018	Finance	L Pettit	Autumn 2020

St Mary's Catholic Primary School, Ipswich

ACCEPTABLE USE AGREEMENT FOR STAFF, GOVERNORS AND VISITORS

This agreement applies to all online use and to anything that may be downloaded or printed.

All adults within the school must be aware of their safeguarding responsibilities when using any online technologies, such as the internet, E-mail or social networking sites. They are asked to sign this Acceptable Use Agreement so that they provide an example to children and young people for the safe and responsible use of online technologies. This will educate, inform and protect adults so that they feel safeguarded from any potential allegations or inadvertent misuse themselves.

- I know that I must only use the school equipment in an appropriate manner and for professional uses.
- I know that I must not use the school devices for personal use unless this has been agreed by the Headteacher.
- I understand that media is only to be uploaded online to the school learning platform unless permission is obtained from the Headteacher.
- I know that images should not be inappropriate or reveal any personal information of children.
- I will report any concerns misuse or virus infection to the Headteacher.
- I will report accidental misuse to the Headteacher
- I will report any incidents of concern for a child or young person's safety to the Headteacher, Senior Designated Person
- I know who my Senior Designated Person is.
- I know that I am putting myself at risk of misinterpretation and allegation should I contact parents/carers or children and young people via personal technologies.
- I will not associate myself online with parents/carers or children linked to St Mary's Catholic Primary. I will not allow children or parents / carers to add me as friends nor will I add them as friends.
- The school asks that you did not identify us as your place of employment
- In line with safeguarding procedures, no comments should be made on social network sites with reference to the school, its governors, pupils, families or any persons associated with it.
- I will ensure that I follow the Data Protection Act 2018 and have checked I know what this involves.
- I will ensure that I keep my password secure and not disclose any security information unless to appropriate personnel. If I feel someone inappropriate requests my password I will check with the e-Safety Lead prior to sharing this information.
- I will adhere to copyright and intellectual property rights.
- I will only install hardware and software I have been given permission for.

- I accept that the use of any technology designed to avoid or bypass the school filtering system is forbidden. I understand that intentional violation of this rule may result in disciplinary procedures being initiated.
- I have been given a copy of the Acceptable Use Policy to refer to about all e-safety issues and procedures that I should follow.
- I will not perform any actions using any technologies that will bring the school into disrepute.

I have read, understood and agree with these Agreement as I know that by following them I have a better understanding of e-Safety and my responsibilities to safeguard children and young people when using online technologies.

Signed…….Date…….

Name (printed)…….

School/……