




# ICT AND INTERNET SAFETY POLICY

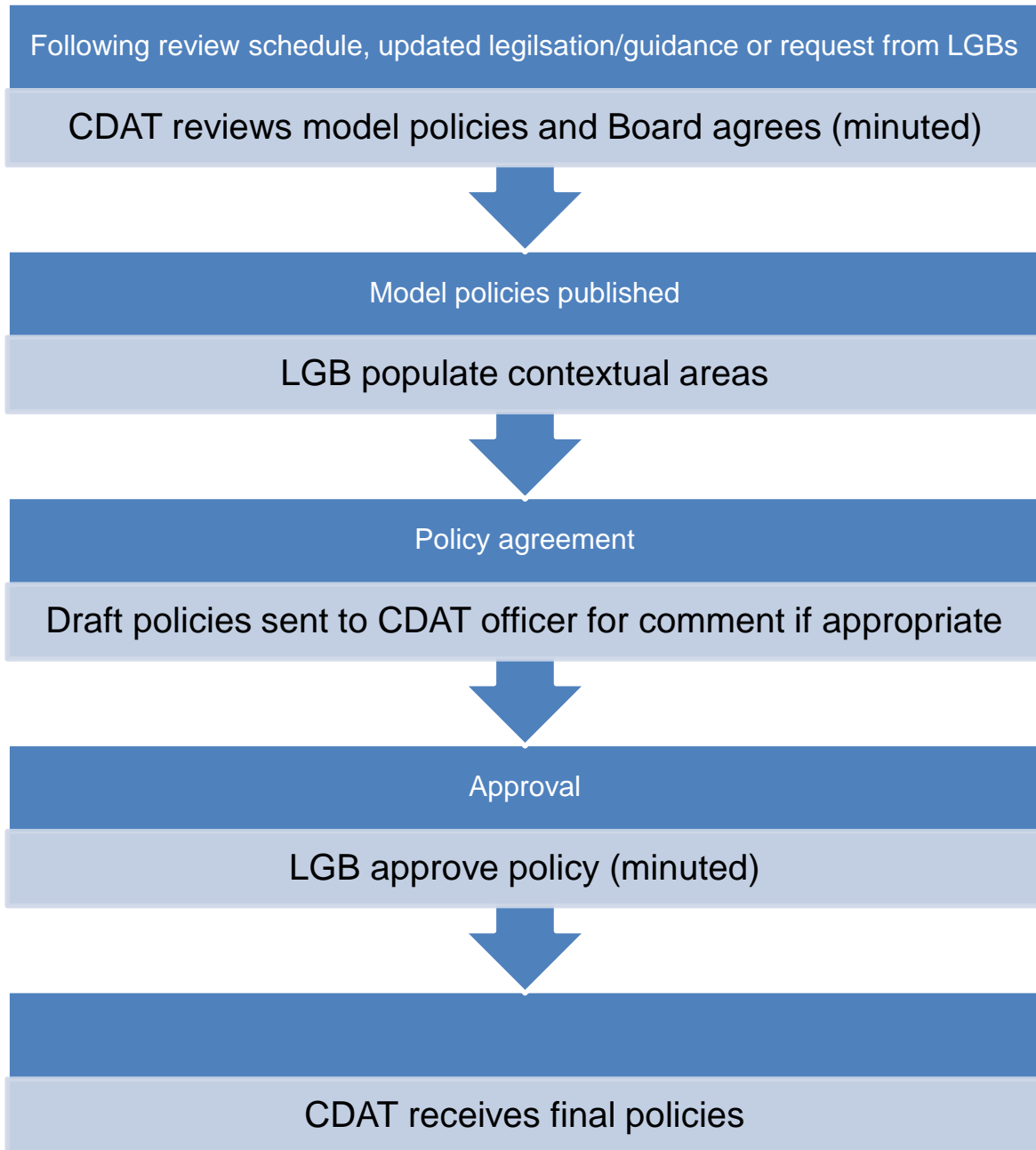
This policy is informed by the Christian values which are the basis for all of CDAT's work and any actions taken under this policy will reflect this.

*'Blessed are those who act justly, who always do what is right'*  
*Psalm 106:3*

**School/Academy Name: St Matthew's C of E Primary**

Date agreed by LGB	Review Date	Signed Chair of LGB
July 2018	Summer 2022	

## Policy Process



## Contents

1. Introduction .....	4
2. Using the internet for learning in academies.....	4
3. Evaluating internet content .....	4
4. Internet use by staff .....	4
5. E-mail.....	5
6. Published content and the academy website.....	5
7. Publishing pupils' images and work .....	5
8. Communication technologies – including chat, forums, blogs, instant messaging services and social networking sites.....	5
9. Mobile phones and other handheld devices (including those that are internet-enabled) .....	6
10. Electronic communications with children by staff.....	6
11. Downloads .....	6
12. Managing filtering .....	6
13. Managing emerging technologies, video-conferencing and electronic resources for learning.....	6
14. Online bullying and harassment (cyberbullying) .....	7
15. Authorising internet access .....	7
16. Assessing risks .....	7
17. Handling e-safety complaints .....	7
18. Introducing the e-safety policy to pupils .....	7
19. Staff and the e-safety policy .....	7
20. Parental support .....	8
21. Local Governing Body (LGB) .....	8
Appendix 1 - Acceptable Use Agreement: Pupils - Primary.....	9
Appendix 2 - Acceptable Use Agreement: Staff, Governors and Visitors .....	10

## 1. Introduction

CDAT understands that computer technology is an essential resource for supporting teaching and learning. The internet, and other digital and information technologies, open up opportunities for pupils and play an important role in their everyday lives.

Whilst CDAT recognises the importance of promoting the use of computer technology throughout the curriculum, it also recognises the need for safe internet access and appropriate use.

CDAT has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff in each academy.

St Matthew's is committed to providing a safe learning and teaching environment for all pupils and staff, and has implemented important controls to prevent any harmful risks.

## 2. Using the internet for learning in academies

All pupils are taught how to find appropriate information on the internet and how to ensure, as far as possible, that they understand who has made this information available and how accurate and truthful it is.

Teachers carefully plan all internet-based teaching and lessons to ensure that pupils are focused and using appropriate and relevant materials.

Children are taught how to use search engines and how to evaluate internet-based information as part of the ICT curriculum, and in other curriculum areas where necessary. They are taught what internet use is acceptable and what is not and given clear objectives for internet use.

Pupils in Key Stage 1 will not be permitted to 'free-surf' the web. In Key Stage 1 and typically in Key Stage 2, pupils' internet access will be through a selection of evaluated sites suitable for the purposes of the task. Processes are in place for dealing with any unsuitable material that is found during internet use.

Where pupils are allowed to freely search the internet, e.g. using search engines, staff are vigilant in monitoring the content of the websites the young people visit. Pupils who need to search individually will be in the upper primary years. Teachers, wherever possible, will have viewed the content prior to use to check its relevance and suitability.

St Matthew's internet access includes filtering, appropriate to the age of the pupils, which is provided by an approved supplier.

## 3. Evaluating internet content

St Matthew's will ensure that staff and pupils are mindful of copyright regulations when copying, downloading and representing materials from the internet. Web-based resources have similar copyright status to printed and recorded materials, such as books, films and music, and this must be taken into consideration when using them. Pupils will be taught to acknowledge the source of information used and to respect copyright when using internet material in their own work.

In Key Stage 2, pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Pupils will be taught how to carry out simple checks for bias and misinformation.

## 4. Internet use by staff

CDAT understands that the internet is a valuable resource for school staff. It provides a wealth of resources, teaching materials and information that we can use to support and enhance learning. It allows staff to share resources with other academies, and to engage in debate and discussion on educational topics and news.

It also provides an efficient way to access information from the Department for Education and other government agencies and departments that will help staff to keep abreast of national and local developments.

There are also increasing opportunities for staff to access INSET and continuing professional development activities using the internet and e-learning resources.

CDAT is committed to encouraging and supporting school/academy staff to make the best use of ICT and all the opportunities it offers to enhance our teaching and support learning.

Staff use of the internet on school computers will be responsible and legal at all times and in keeping with their professional role and responsibility. Misuse of the internet and school computer systems will be rigorously investigated and could lead to disciplinary action being taken.

## **5. E-mail**

E-mail is one of the many modes of communication that plays an important role in many aspects of our lives today. St Matthew's teaches the use of e-mail as part of the ICT curriculum to educate children to be aware of the benefits and risks and how to be safe and responsible users as part of e-safety provision.

Pupils are taught strategies to deal with inappropriate emails and are reminded of the need to write emails clearly and correctly, not including any unsuitable or abusive material. Pupils are taught not to reveal personal details of themselves or others in e-mail communication, nor to arrange to meet anyone without specific permission.

Staff must use the school email service and accounts that are available for professional communication. They are more secure and are easier to access by a third party should the need for scrutiny arise.

Staff should always ensure that they represent the school in a professional and appropriate way when sending e-mail, contributing to online discussions or posting to public websites. Failure to do so could lead to disciplinary action being taken.

## **6. Published content and the school website**

Contact details on the school's web site will be the school address, e-mail and telephone number. Individual, personal contact information will not be published.

The principal will take overall editorial responsibility and ensure that content is accurate and appropriate. It will be the responsibility of other staff, personally or by delegation, to update the website regularly.

## **7. Publishing pupils' images and work**

The development of digital imaging technologies has created significant benefits to learning, giving staff and pupils instant use of images and video that they have recorded themselves or downloaded from the internet. However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images / video on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm.

Staff are allowed to take digital / video images to support educational aims, but must follow the school's policy concerning the sharing, distribution and publication of those images which states that:

- care should be taken when taking digital / video images that students / pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school/academy into disrepute or danger;
- nobody should take, use, share, publish or distribute images of others without their permission;
- photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images;
- pupils' full names will not be used anywhere on the website or learning platform, particularly in association with photographs;
- parents or carers are informed of our policy on publishing and are able to opt their children out.

## **8. Communication technologies – including chat, forums, blogs, instant messaging services and social networking sites**

Most of these modes of electronic communication are restricted in the school; however, they are being used more frequently by pupils and staff outside of school.

We acknowledge social networking sites, blogs, instant messaging services, chat rooms and forums are beneficial for communication, learning and research. They also present a range of personal safety and privacy issues.

During school time, pupils and staff are not permitted to access social networking sites, public chat rooms, discussion groups and forums etc. using school resources. Most are blocked by the filtering service used by the school.

## **9. Mobile phones and other handheld devices (including those that are internet-enabled)**

It is anticipated that more pupils will have access to internet-enabled devices such as mobile phones or other handheld devices, which are capable of browsing and uploading to the internet, accessing email and social networking services, as well as taking photos and recording video.

St Matthew's recognises the potential advantages these devices can offer for staff and pupils and there are clear and enforceable rules for their use.

Pupils are taught the legal and moral implications of posting photos and personal information from mobile phones to public websites and how to use these technologies in a safe and responsible manner.

Children must not bring mobile phones to school. Only in exceptional, prior arranged circumstances, will the school permit mobile phones belonging to pupils on the premises. If such a set of circumstances is deemed necessary, the mobile phone will be kept securely in the school office.

Staff should represent the school in a professional and appropriate way when communicating via the internet, contributing to online discussions or posting to public websites using school facilities.

## **10. Electronic communications with children by staff**

Communication between children and school staff should take place within clear and explicit professional boundaries.

Staff must be careful not to share any personal information with children such as email, web-based communication facilities, home or mobile numbers. They should not request, or respond to, any personal information from the child / young person, other than that which might be appropriate as part of their professional role.

Staff should ensure that all communications are transparent and open to scrutiny. In addition, all staff must use social networking in an appropriate manner and uphold professional confidentiality at all times. Staff should not accept parents or pupils as 'friends' on social contact sites such as Facebook.

## **11. Downloads**

Pupils must not be allowed to download any material from the internet on to school computers unless directed to do so by an appropriate staff member.

Staff should take care that files from both other computers outside the school and internet are checked for virus contamination before they are used on the school system.

Pupils are not allowed to use CDs, DVDs or memory sticks brought from home unless they have been given permission.

St Matthew's subscribes to suitable antivirus software. The software is updated regularly.

## **12. Managing filtering**

Whilst filtering technology is robust and generally effective at blocking unsuitable material, it is still possible for unsuitable material to occasionally get past the filter. Pupils are taught to always report such experiences directly to an adult at the time they occur, so that action can be taken.

The action will include:

- making a note of the website and any other websites linked to it;
- informing the ICT leader and principal;
- logging the incident;
- informing the internet service provider so that the website can be added to the content filter if appropriate;
- discussion with the pupil about the incident, and how they might avoid similar experiences in future;
- parents being informed, where necessary.

Pupils or staff who deliberately try and access unsuitable materials will be dealt with in accordance with the school's discipline policies for pupils and staff.

## **13. Managing emerging technologies, video-conferencing and electronic resources for learning**

Emerging technologies and resources will be examined for educational benefit and a risk assessment will be carried out before use in the school is permitted.

#### **14. Online bullying and harassment (cyberbullying)**

Online bullying and harassment via instant messaging, chat rooms, social networking sites etc. are potential problems that can have an effect on the wellbeing of pupils and staff alike.

There is a range of strategies and policies in place to prevent online bullying. These include:

- allowing no access whilst at school to public chat-rooms, instant messaging services and social networking sites;
- pupils being taught how to use the internet safely and responsibly which includes how to identify and respond to 'cyberbullying';
- children being taught how and where to report incidents that make them feel unhappy or worried;
- pupils being encouraged (as with all forms of bullying) to discuss with staff any concerns or worries they have about online bullying and harassment.

#### **15. Authorising internet access**

All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource.

The school will keep a record of all staff and pupils who are granted internet access. The record will be kept up-to-date, for instance a member of staff may leave or a pupil's access be withdrawn.

At Key Stage 1, access to the internet will be by adult demonstration with occasional, directly supervised, access to specific, approved on-line materials. Parents are asked to sign and return a consent form when their child starts at St Matthew's.

#### **16. Assessing risks**

The school will take all reasonable precautions to ensure that users access only appropriate material; however, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer.

St Matthew's can't accept liability for the material accessed, or any consequences of internet access.

St Matthew's will audit ICT provision (including system and security) regularly to establish if the e-safety policy is adequate and that its implementation is effective.

#### **17. Handling e-safety complaints**

Any complaint about staff misuse must be referred to the principal.

Complaints of a child protection nature must be dealt with in accordance with the child protection procedures.

Pupils and parents will be informed of the complaints procedure.

#### **18. Introducing the e-safety policy to pupils**

E-safety rules will be posted in all networked rooms and discussed with the pupils at the start of each year. Pupils will be informed that network and internet use can be monitored.

#### **19. Staff and the e-safety policy**

All staff will be given access to the school's E-Safety Policy and its importance will be explained.

A programme of e-safety training will be available to staff, who can also discuss matters with the e-safety coordinator on an ad-hoc basis.

Staff should be aware that internet traffic can be monitored and traced to the individual user.

Discretion and professional conduct is essential.

All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school's Acceptable Use Policy.

The e-safety coordinator will receive regular updates through attendance at training sessions and / or by reviewing guidance documents released by appropriate authorities and providers.

## 20. Parental support

Some parents and carers might have a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of children's on-line experiences.

Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it.

St Matthew's provides information and awareness to parents and carers through:

- information in newsletters;
- links to resources from the website;
- parent workshops.

## 21. Local Governing Body (LGB)

LGB members should take part in e-safety training / awareness sessions, with particular importance for those who are members of any sub-committee / group involved in ICT / e-safety / health and safety / safeguarding.

They should also sign the Acceptable Use Agreement.



## Appendix 1 - Acceptable Use Agreement: Pupils - Primary

### Primary Pupil Acceptable Use Agreement / e-Safety Rules

- I will only use ICT in school for school purposes;
- I will only use my class email address or my own school email address when emailing;
- I will only open email 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 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 or 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 upload or add any images, video, sounds or text that could upset any member of the school/academy community;
- I know that my use of ICT can be checked and my parent/carer contacted if a member of 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 sign up to online services until I am old enough.

Dear parent/carer

ICT, including the internet, email 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 e-safety 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 your child's class teacher.

Please take care to ensure that appropriate systems are in place at home to protect and support your child/ren.

✂

---

#### Parent/ carer signature:

We have discussed this document with .....(child's name) and we agree to follow the e-safety rules and to support the safe use of ICT at St Matthew's C of E Primary School.

Parent/carer signature .....

Class ..... Date .....

## Appendix 2 - Acceptable Use Agreement: Staff, Governors and Visitors

### Staff, Governor and Visitor

#### Acceptable Use Agreement / Code of Conduct

ICT (including data) and the related technologies such as email, the internet and mobile devices, are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the ICT coordinator.

- I will only use the school's email / internet / intranet / learning platform and any related technologies for professional purposes or for uses deemed acceptable by the principal or Local Governing Body (LGB);
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities;
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role;
- I will not give out my own personal details, such as mobile phone number, personal email address, personal Twitter account, or any other social media link, to pupils;
- I will only use the approved, secure email system(s) for any school business;
- I will ensure that personal data (such as data held on MIS software) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the principal or LGB. Personal or sensitive data taken offsite must be encrypted, e.g. on a password secured laptop or memory stick;
- I will not install any hardware or software without the permission of the business manager;
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory;
- Images of pupils and / or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member;
- Images will not be distributed outside the school network without the permission of the parent / carer, member of staff or principal;
- I will support the school's approach to online safety and not upload or add any images, video, sounds or text linked to or associated with St Matthew's or its community without the permission of the principal or LGB;
- I understand that all my use of the internet and other related technologies can be monitored and logged and can be made available, on request, to my line manager or the principal;
- I will respect copyright and intellectual property rights;
- I will ensure that my online activity, both inside and outside school, will not bring St Matthew's, CDAT, my professional reputation, or that of others, into disrepute;
- I will support and promote the school's e-safety and data security policies and help pupils to be safe and responsible in their use of ICT and related technologies;
- I will not use personal electronic devices in public areas of the school between the hours of 8.30am and 3.30pm, except in the staff room and where there are signs to indicate this.

#### User signature

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

Signature ..... Date .....

Full name ..... (printed)

Job title .....