St Mary's Catholic Primary School

ICT Policy including Acceptable Use of ICT for pupils

This policy should be read in conjunction with other policies including Behaviour, Anti-Bullying, Safeguarding, Social Media Policy, Staff Acceptable Use of ICT Policy and RHE. Throughout the policy, 'Computing' is used to refer to the specific curriculum subject and 'ICT' to describe the broader use of technology.

Introduction

ICT equipment and resources within our school are provided to enhance pupils' learning and to aid staff in their delivery of the curriculum. These guidelines have been written to ensure that everyone in the school is aware of what is expected of them and can stay safe when using this hardware and software. This policy sets out a framework for how computing as a subject will be taught in school and how general use of ICT will be monitored. Further information on the different systems in school will be made available to staff.

Aims

We believe that it is important for children, staff and the wider school community to have the confidence and ability to use ICT tools to prepare them for an ever-changing and rapidly developing world. To enable all our staff and pupils to be confident, competent, independent and safe users and learners of Computing we aim:

- To use ICT where appropriate to ensure pupils are motivated and inspired in all areas of the curriculum.
- To use ICT to help improve standards in all subjects across the curriculum.
- To develop the ICT competence and skills of pupils through computing lessons and provide them with the chance to consolidate these in a cross-curricular context.
- To ensure pupils are challenged in their use of ICT and are provided with exciting, creative ways in which to share their learning.
- To use tools available to ensure children have the ability to work independently and collaboratively to suit the needs of the situation.
- To provide all staff with the training and support to ensure that they can, and have the confidence to, use ICT to its full potential in all aspects of school life.
- To use ICT as a form of communication with parents, pupils and the wider community.

Curriculum

Computing will be taught across the curriculum and, wherever possible, integrated into other subjects applying skills that have been learnt in computing sessions. Our computing curriculum document shows the learning journey which the children are expected to take. The computing curriculum lead will ensure that the plans provide a broad and progressive development of skills using appropriate software.

Online Learning

As a school, we value the importance of providing opportunities for children to learn outside of school and we will provide these depending on the age of the child.

For children in Foundation Stage and Key Stage 1, we will:

- Provide links from the school website to websites suitable for the age group.
- Provide a personal login to Purple Mash.

For Key Stage 2 children, we will:

- Provide links from the school website to websites suitable for the age group.
- Provide a personal login to Purple Mash.
- Provide personal logins to other services such as Reading Plus and Timestable Rockstars.

Assessment

Computing will be assessed in a number of ways using formative and summative assessment. Formative assessment will happen during computing lessons and will be used to inform future planning and this is conducted by the teacher on an informal basis. Children will store their work on Purple Mash and their own personal Microsoft 365 account which enables staff to view a child's complete portfolio and make summative judgements.

Equal Opportunities and Inclusion

We will ensure that all pupils are provided with opportunities to access the computing curriculum throughout the school. Where necessary, we will endeavour to make adaptations to the environment or provide software that will enable all learners to achieve. Homework completion will not be dependent in access to the internet at home.

Roles and Responsibilities - The School

As a school we will endeavour to ensure that parents and pupils are fully aware of ways in which the internet and ICT can be used productively and safely. We will always ensure that we provide children with the opportunities to excel and achieve when using ICT and will ensure our curriculum is challenging and relevant. Before launching any system or initiative, we will make sure that the children's safety is at the forefront of our thoughts, and we will keep parents informed as necessary through newsletters and curriculum events.

Roles and Responsibilities – Computing subject lead

The computing subject lead will oversee planning in all year groups throughout the school and be responsible for raising standards in computing and ICT. They will also be responsible for informing staff of new developments and initiatives and providing training where appropriate. The computing subject lead is responsible for overseeing the assessment of computing across the school. They are also responsible for working alongside the school business manager and Headteacher to oversee software licensing, managing equipment, providing guidance for future purchasing and ensuring that procedures are sustainable.

Roles and Responsibilities - Teachers

Class teachers are responsible for planning, teaching and recording pupil progress in computing in accordance with guidance provided by the computing subject lead. Teachers are also responsible for using

ICT on an everyday basis with their class, including the use of the interactive white board to provide visual stimulus for learning and providing opportunities to use audio visual equipment. Teachers should respond to and report any e-safety or cyberbullying issues that they encounter within or out of school in accordance to e-safety procedures in the Acceptable Use Policy. Staff must adhere to the Staff Acceptable Use Policy (AUP) and Code of Conduct.

Roles and Responsibilities - Pupils

Pupils should follow the guidelines laid out in the ICT Acceptable Use Policy for Pupils. They should ensure that they use the computers and equipment appropriately at all times. It is expected that children will follow the school's Behaviour Policy when working online. They are also expected to adhere to the school's Anti-Bullying Policy. If the children fail to do so, then the procedures outlined in these policies will be applied.

Roles and Responsibilities - Parents

Parents are asked to support the school in ensuring adherence to the Acceptable Use Policy for pupils and to discuss this with their child. Parents should stay vigilant to the websites and content that their children are accessing and try to talk to their child about e-safety and the use of the internet. If they have any questions or concerns then they should speak to their child's teacher, a Designated Safeguarding Lead or the Headteacher.

Roles and Responsibilities - Governors and Visitors

School governors should abide by the guidelines set out for staff and ensure that any use of computers and equipment within school is carried out in accordance with this. If either a visitor or governor wishes to have a temporary account to logon to the school network, they should speak to the Headteacher or school business manager.

Equipment - Hardware and Software

ICT equipment should be used with care to preserve life and prevent wastage. To promote this, no food and drink is allowed near equipment in the classroom. Communal resources such as cameras and microphones should be returned after use with files removed and wastage of batteries, printer ink and paper minimised. Hardware should not be installed without the permission of the Headteacher. Staff must not use any computer hardware from outside school. The installation of software unauthorised by the school, whether licensed or not, is forbidden. The school reserves the right to examine or delete any files that are held on its system.

Sustainability and Environmental Impact

Hardware is disposed of safely and securely in accordance with WEEE.

Network

Accounts on the network are created and monitored by the BWCET IT services. Staff are issued with a username for the network and a temporary password which needs to be changed in accordance with the password procedure below. Children have individual logins based on their full name as given in Arbor except where variations are requested by class teachers prior to the creation of logins. Usernames and passwords will be required to access the school's network. Pupils will also be issued with usernames and passwords for online services. The computing subject lead will liaise with IT services to ensure usernames

and passwords are issued for new pupils. Once they have left our school, the child's account and their content will be removed. Pupils, staff and other visitors must not attempt to access the school's Wi-Fi on a personal device.

Passwords

BWCET IT services hold the passwords to different areas of the school network and have administrator access. Users will be given access to systems at the appropriate level. All staff have password protected access to the school network and the initial password must be changed at first login. Staff should make sure that any passwords they use are strong and contain a mixture of some of the following; upper- and lower-case letters, numbers and punctuation. These should be changed regularly, especially if the user suspects others may know the password. Staff should be aware of and apply the guidance given in the Staff AUP with regard to data security. For online services used in school such as Oxford Owl, there is a school password which allows staff to access the assessment manager area. It is important that these details are not accessible to pupils at any point. For sites such as Purple Mash, Reading Plus and Timestable Rockstars, children have personal passwords. These passwords are site-specific and as children progress through the school they will be taught about choosing sensible and secure passwords for online sites and apps.

Backups

The data stored on the school's network is backed up on site and remotely. Staff need to notify IT services immediately if they realise something has been accidently deleted so that copies of files can be recovered.

School Website

The school website is managed by BWCET IT services and the Headteacher. All classes can submit documents and photographs for publication. Photographs including images of children need to be checked for parental permission and meet the criteria shown below before submission.

Digital and Video Images

As a school we will ensure that if we publish any photographs or videos of children online, we will:

- Ensure that their parents or guardians have given us written permission.
- Ensure if we do not have permission to use the image of a particular child, we will make them unrecognisable to ensure that they are not left out of situations unnecessarily.
- Not include a child's image and their full name together without permission from the parents or guardians (e.g. if the child has won an award).
- Ensure that children are in appropriate dress.
- Remove photos at the request of a parent, guardian or child. This request can be made verbally or in writing to the Headteacher. We will endeavour to remove the photograph as soon as possible.
- Not re-use any photographs or recordings after a child leaves this school.
- Ask parents or guardians who are recording video or taking digital images at public events (e.g. school play or sports day) that they do not publish these online.

Filtering and monitoring

The school has comprehensive filtering and monitoring systems in place. The school is supported by Smoothwall (Durham LA) for filtering and Senso for its monitoring. The Headteacher completes regular monitoring of concerns picked up from Senso. Critical violations will be acted upon as a matter of urgency

in-line with safeguarding procedures. Any 'true positives' will be acted upon and actions recorded for future reference.

Prevent Duty

Schools are expected to ensure children are safe from terrorist and extremist material when accessing the internet in school. This is achieved at St Mary's Catholic Primary School by establishing appropriate levels of filtering. Comprehensive filtering is currently in place which, amongst others, blocks access to social media sites and YouTube.

Internet and E-mail

The internet may be accessed by staff and by children throughout their hours in school and users are responsible for ensuring that they have logged off so that other users cannot access previously accessed sites. Staff need to be vigilant as to the sites children are accessing and children should not be using the internet unattended. The teaching of email, internet use and other aspects of e-safety will be covered within the computing curriculum planning, but staff should encourage regular dialogue that explores the benefits and potential dangers of using the internet. If users, especially children, see an inappropriate website or image, they should minimise the page immediately and report the site to their class teacher who will report this to the Computing subject lead. BWCET IT services will be contacted to attempt to get this site blocked. Children are not currently issued with an individual email address but learn to use email through off-line software. Staff are provided with a school Office 365 email address and need to follow the guidelines in the Staff AUP when using this.

Social Media

As a school we recognise that social media and networking are playing an increasing role within every-day life and that many staff are users of tools such as Facebook, X and blogs for both personal and professional use. We will ensure that staff and children are kept fully aware of risks and issues that may arise and ways in which to minimise these risks. Staff should apply the guidance given in the Staff AUP and Social Media policies with regard to social networking. Pupils should not be signed up to most social networking sites due to the over-13 age limit. However, we recognise that many are signed up either with or without parental knowledge. As a school, we reserve the right to contact sites such as Facebook and ask them to remove our children's accounts should any issues, such as cyberbullying, occur.

E-Safety

We take e-safety seriously and will ensure that computing and PSHE sessions teach how to minimise the risk when working on the internet, managing passwords and respecting copyright, as relevant to the children's age. All children will be taught about the Internet Acceptable Use Policy. Useful ICT rules will also be displayed to ensure they are seen by children and visitors. If a teacher suspects an E-safety issue within school they should make notes related to the incident in accordance with school Anti-bullying and Behaviour policies. This should then be reported to the Computing subject lead and Headteacher, recorded and parents contacted as appropriate.

Cyberbullying

Cyberbullying can be defined as the use of Information and Communications Technology (ICT) deliberately to upset someone else and may involve email, virtual learning environments, chat rooms, social

networking sites, mobile and landline telephones, digital camera images and game and virtual world sites. Through Computing lessons, assemblies and PSHE, children will be taught the SMART rules:

SAFE
Keep safe by being careful not to give out personal information online.

MEETING
Never agree to meet anyone that you chat to on the internet; they may not be who you think they are. You can't be sure who you're talking to on the Internet.

ACCEPTING
Do not accept unusual e-mails. They may be trying to tempt you into opening them. They could contain viruses that can damage your computer. If this happens to you, tell an adult.

RELIABLE
Information on the internet may not be true – anyone can upload material to the internet. Always double check any information on a more reliable website.

TELL
If anything makes you feel worried tell your parents, teachers or an adult that you trust. They can help you to report it to the right place or call a helpline like ChildLine on 0800 1111 in confidence.

Copyright
Copyright of materials should be respected. Staff should check permission rights before downloading material, particularly images from the internet, and/or copying from printed materials. Staff should not remove logos or trademarks unless the terms of the website allow it. Children will be taught that it is not acceptable to take images directly from the internet without permission for use and to start referencing the sites they have used.

Responding to unacceptable use by pupils
Pupils should be aware that all e-safety issues will be dealt with quickly and effectively. When dealing with unacceptable use, staff should follow the Behaviour and Anti-bullying policies as necessary.

Responding to unacceptable use by staff
Failure to comply with the guidelines and expectations in the Staff AUP could lead to sanctions and possible disciplinary action in accordance with the school's policies and the law.

Acceptable Use Policy - Governors and Visitors
Visitors may be provided with accounts to our network and/or online systems on a case-by-case basis, depending on the purpose of the account requested. Users will be expected to follow the guidelines as set out for staff and understand that accounts may be removed at any time.

Complaints
Incidents regarding the misuse of the Internet by students will be forwarded to the Headteacher and Computing subject lead who will decide whether additional evidence should be gathered or recorded. A

partnership approach with parents will be encouraged. Any complaint about staff misuse will be referred to the Headteacher. Complaints of a safeguarding nature must be dealt with in accordance with safeguarding procedures.

Appendix A: Acceptable Use guidance to be shared with pupils

The school has computers with Internet access to help you with your learning. These rules need to be understood before you use the Internet and will help you to keep safe and be fair to others.

Using laptops/computers:

- I will be respectful and careful when using laptops/ computers.
- I will report any damage to computers/ laptops as soon as I am aware of it to a member of staff.
- I will only access the school network with the login I have been given.
- I will not try to access files in other people's folders.
- I will close all programs and log out before leaving the computer.
- I will not use any computer hardware from outside of school (e.g. USB hard drives).

Using ipads:

- I will be respectful and careful when using ipads.
- I will report any damage to ipads as soon as I am aware of it to a member of staff.
- I will only access applications when guided by a member of staff.
- I will not change applications without checking with an adult.
- I will not access the internet without permission.
- I will not use the camera application without guidance from a member of staff, and I will only take photos/videos which a member of staff has guided me to.

Using the Internet:

- I will ask permission from a teacher before using the Internet.
- I will only search the Internet in ways that my teacher has approved.
- I will check who owns an image I may want to use on the Internet and will only use those with permission for re-use.
- I will minimise the web page if I find any unpleasant material and will report this to my teacher immediately because this will help protect other pupils and myself.
- I understand that the school may check my computer files and monitor what I type on my laptop/ computer as well as the Internet sites I visit.

Using e-mail/ messaging /forms:

- I will not give my full name, date of birth, home address or telephone number on any website.
- I will not share anyone else's personal information online.
- I will not use the Internet to arrange to meet someone outside school hours.
- I will ask permission from a teacher before sending any messages on the Internet and will only send messages to people/ sites that my teacher has approved.
- The messages I send will be polite and responsible.
- I will immediately report any unpleasant messages sent to me because this will help protect other pupils and myself.