SS Peter & Paul
Catholic Primary School

Policy on
E-Safety

Policy Written & Agreed: _____

Ratified by Full Governing Body: _____September 2020_____

To be reviewed: _____September 2021_____

SS Peter & Paul
Whole School Policy on E-Safety

This E-Safety policy:-
- is based on Local Authority Model Policy guidance – September 2014
- reflects the consensus of opinion of the whole staff;
- was discussed, written and agreed by the whole staff;
- has been approved by the Governing body.

The implementation and ownership of this policy is the responsibility of the whole staff.

The overall accountability and effectiveness of the policy will be the responsibility of the Head Teacher and Senior Leadership Team.

At SS Peter & Paul Catholic Primary School we take a professional and pro-active approach to E-Safety and we are committed to keeping our children safe both in and out of School. As a Catholic school, we believe all are created in the image and likeness of God and should be protected from harm of any description.

1.0 INTRODUCTION

1.1 At SS Peter & Paul, we understand 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.

1.2 Whilst we recognise the importance of promoting the use of computer technology throughout the curriculum, we also recognise the need for safe internet access and appropriate use. Our school 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.

1.3 The school 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. This policy will operate in conjunction with other important policies in our school, including our 'Anti-bullying Policy', 'Data Protection Policy', 'Safeguarding Policy' and 'Acceptable Use of the Internet & Technology Policy'.

2.0 USE OF THE INTERNET

2.1 The school understands that using the internet is important when raising educational standards, promoting pupil achievement and enhancing teaching and learning.

2.2 Internet use is embedded in the statutory curriculum and is therefore entitled to all pupils, though there are a number of controls required for schools to implement, which minimise harmful risks.

2.3 When accessing the internet, individuals are especially vulnerable to a number of risks which may be physically and emotionally harmful. These risks include:
- Access to illegal, harmful or inappropriate images
- Cyber bullying
- Access to, or loss of, personal information
- Access to unsuitable online videos or games
- Loss of personal images
- Inappropriate communication with others
- Illegal downloading of files
- Plagiarism and copyright infringement
- Sharing the personal information of others without the individual's consent or knowledge

3.0 ROLES & RESPONSIBILITIES

3.1 It is the responsibility of all staff to be alert to possible harm to pupils or staff, due to inappropriate internet access or use both inside and outside of the school, and to deal with incidents of such as a priority.

3.2 The e-safety officer, Teresa Wright (Computing Co-ordinator), supported by Martin Latham (Link2ict), is responsible for ensuring the day-to-day e-safety in our school, and managing any issues. The head teacher is responsible for ensuring that the e-safety officer and any other relevant staff receive continuous professional development to allow them to fulfil their role and train other members of staff.

3.3 The e-safety officer will provide all relevant training and advice for members of staff on e-safety.

3.4 The head teacher will ensure there is a system in place which monitors and supports the e-safety officer, whose role is to carry out the monitoring of e-safety in the school. The e-safety officer will regularly monitor the provision of e-safety in the school and return this to the head teacher. The school will establish a procedure for reporting incidents and inappropriate internet use, either by pupils or staff and ensure that all members of staff are aware of the procedure when reporting e-safety incidents, and will keep a log of all incidents recorded.

3.5 Cyber bullying incidents will be reported in accordance with the school's Anti-Bullying Policy.

3.6 The governing body will hold regular meetings with the head teacher and/or e-safety officer to discuss the effectiveness of the e-safety provision, current issues, and to review incident logs. The governing body will evaluate and review this E-safety Policy on an annual basis. The head teacher will review and amend this policy with the e-safety officer, taking into account new legislation and government guidance, and previously reported incidents to improve procedures.

3.7 Teachers are responsible for ensuring that e-safety issues are embedded in the curriculum and safe internet access is promoted at all times. All staff are responsible for ensuring they are up-to-date with current e-safety issues, and this E-safety Policy.

3.8 All staff and pupils will ensure they understand and adhere to the 'Acceptable Use of the Internet Policy', which they must sign as part of their 'Code of Conduct' and return to the head teacher.

3.9 Parents/carers are responsible for ensuring their child understands how to use computer technology and other digital devices, appropriately. The head teacher is responsible for communicating with parents regularly and updating them on current e-safety issues and control measures.

4.0 E-SAFETY CONTROL MEASURES

4.1 Educating pupils:
- An e-safety programme will be established and taught across the curriculum on a regular basis, ensuring pupils are aware of the safe use of new technology both inside and outside of the school.
- Pupils will be taught about the importance of e-safety and are encouraged to be critically aware of the content they access online.
- Pupils will be taught to acknowledge information they access online, in order to avoid copyright infringement and/or plagiarism.
- Clear guidance on the rules of internet use will be presented in all classrooms.
- Pupils are instructed to report any suspicious use of the internet and digital devices.

4.2 Educating staff:
- All staff will undergo e-safety training on a termly basis to ensure they are aware of current e-safety issues and any changes to the provision of e-safety.
- All staff will undergo regular audits by the e-safety officer in order to identify areas of training need.
- All staff will employ methods of good practice and act as role models for pupils when using the internet and other digital devices.
- Any new staff are required to undergo e-safety training as part of their induction programme, ensuring they fully understand the E-safety Policy.

4.3 Internet access:
- Internet access will be authorised once parents and pupils have returned the signed consent form as part of the Acceptable Use of the Internet Policy.
- A record will be kept by the head teacher of all pupils who have been granted internet access.
- All users in key stage 2 and above will be provided with usernames and passwords, and are advised to keep this confidential to avoid any other pupils using their login details.
- Pupils' passwords will be changed on a regular basis, and their activity is continuously monitored by the e-safety officer.
- Management systems will be in place to allow teachers and members of staff to control workstations and monitor pupils' activity.
- Effective filtering systems will be established to eradicate any potential risks to pupils through access to particular websites.
- Any requests by staff for websites to be added or removed from the filtering list must be first authorised by the head teacher.
- All school systems will be protected by up-to-date virus software.
- An agreed procedure will be in place for the provision of temporary users, e.g. volunteers.
- The master users' passwords will be available to the head teacher for regular monitoring of activity.

4.4 E-mail:
The school e-mail system is provided, filtered and monitored by Link2ICT and is governed by Birmingham City Council's E-mail Use Policy:
- Pupils and staff will be given approved email accounts and are only able to use these accounts.
- Use of personal e-mail to send and receive personal data or information is prohibited.
- No sensitive personal data shall be sent to any other pupils, staff or third parties via email.
- Any emails sent by pupils to external organisations will be overseen by their class teacher and must be authorised before sending.
- Chain letters, spam and all other emails from unknown sources will be deleted without opening.

4.5 Social Networking:
- Access to social networking sites will be filtered as appropriate.
- Should access be needed to social networking sites for any reason, this will be monitored and controlled by staff at all times and must be first authorised by the head teacher.
- Pupils are regularly educated on the implications of posting personal data online, outside of the school.
- Staff are regularly educated on posting inappropriate photos or information online, which may potentially affect their position and the [school/academy] as a whole.
- Staff are not permitted to communicate with pupils over social networking sites.

4.6 Published content on the school website and images:
- The head teacher will be responsible for the overall content of the website, and will ensure the content is appropriate and accurate.
- All contact details on the [school/academy] website will be the phone, email and address of the school. No personal details of staff or pupils will be published.
- Images and full names of pupils, or any content that may easily identify a pupil, will be selected carefully, and will not be posted until authorisation from parents has been received.
- Pupils are not permitted to take or publish photos of others without permission from the individual.
- Staff are able to take images, though they must do so in accordance with school policies in terms of the sharing and distribution of such. Staff will not take images using their personal equipment.

4.7 Mobile devices:
- The head teacher may authorise the use of mobile devices by a pupil where it is seen to be for safety or precautionary use.
- Mobile devices are not permitted to be used in the classroom by pupils or members of staff.
- The sending of inappropriate messages or images from mobile devices is prohibited.
- Mobile devices must not be used to take images of pupils or staff.
- The school will be especially alert to instances of cyber bullying and will treat such instances as a matter of high priority.

4.8 Digital Media:

We respect the privacy of the school community and will obtain written permission from staff, parents, carers or pupils before any images or video are published or distributed outside the school.

- Photographs will be published in-line with the Child Protection Act and not identify any individual pupil.
- Students' full names will not be published outside the school environment.
- Permission will be obtained from parents or carers prior to pupils taking part in external video activities.

5.0 <u>SECURITY</u>

5.1 The school endeavours to provide a safe environment for the whole community and we review both physical and network security regularly and monitor who has access to the system consulting with the LA where appropriate.

5.2 Anti-virus software is installed on all computers and updated regularly.

5.3 Central filtering is provided and managed by Link2ICT. All staff, students, visitors, supply teachers are made aware of this and understand that if an inappropriate site is discovered it must be reported to the e-Safety co-ordinator who will report it to the Link2ICT Service Desk to be blocked. All incidents will be recorded in the e-Safety log for audit purposes.

5.4 Requests for changes to the filtering will be directed to the e-Safety co-ordinator in the first instance who will forward these on to Link2ICT or liaise with the Head as appropriate. Change requests will be recorded in the e-Safety log for audit purposes

5.5 The school uses Policy Central Enterprise on all school owned equipment to ensure compliance with the Acceptable Use Policies.
- Pupils use is monitored by Mrs Teresa Wright.
- Staff use is monitored by the Mr Neil Porter.

5.6 All staff, visitors and supply teachers are issued with their own username and password for network access.

5.7 All pupils are issues with their own username and password and understand that this must not be shared.

6.0 <u>CYBER-BULLYING</u>

6.1 For the purpose of this policy, "cyber bullying" is a form of bullying whereby an individual is the victim of harmful or offensive posting of information or images, online.

6.2 The school recognises that both staff and pupils may experience cyber bullying and will commit to preventing any instances that should occur.

6.3 The school will regularly educate staff, pupils and parents on the importance of staying safe online, as well as being considerate to what they post online.

6.4 The school will commit to creating a learning and teaching environment which is free from harassment and bullying, ensuring the happiness of all members of staff and pupils.

6.5 The school has zero tolerance for cyber bullying, and any incidents will be treated with the upmost seriousness and will be dealt with in accordance with our Anti-bullying Policy.

6.6 The head teacher will decide whether it is appropriate to notify the police or anti-social behaviour co-ordinator in their Local Authority of the action taken against a pupil.

7.0 REPORTING MISUSE

Misuse by pupils:
- Teachers have the power to discipline pupils who engage in misbehaviour with regards to internet use.
- Any instances of misuse should be immediately reported to a member of staff, who will then report this to the head teacher, using a complaints form.
- Any pupil who does not adhere to the rules outlined in our Acceptable Use of the Internet Policy and is found to be wilfully misusing the internet, will have a letter sent to their parents/carers explaining the reason for suspending their internet use.
- Members of staff may decide to issue other forms of disciplinary action to a pupil upon the misuse of the internet. This will be discussed with the head teacher and will be issued once the pupil is on the school premises.
- Complaints of a child protection/safeguarding nature shall be dealt with in accordance with our 'Safeguarding Policy'.

Misuse by staff:
- Any misuse of the internet by a member of staff should be immediately reported to the head teacher, using a complaints form.
- The head teacher will deal with such incidents in accordance with the Allegations Against Staff section of our 'Safeguarding Policy', and may decide to take disciplinary action against the member of staff.
- The head teacher will decide whether it is appropriate to notify the police or anti-social behaviour co-ordinator in their Local Authority of the action taken against a member of staff.

Policy Written & Agreed: _____

Ratified by Full Governing Body: ____September 2020_____

To be reviewed: ____September 2021_____

<u>BGFL 365 User Agreement for Pupils</u>

To the children of SS Peter & Paul Catholic Primary School:

You now have use of the school's BGfL 365 accounts and the variety of tools BGfL 365 provides. This means you will be able to access your work in school and at home on a range of devices, this offers huge advantages to help with your learning. With this, come the potential risks involved when using online technologies and something you need to learn about in this safe environment.

You need to use technology **Safely, Responsibly and Respectfully**. We are a caring school and take our role in making the internet a safer place for everyone, by looking out for each other. We will be learning about Online Safety in our lessons at school.

Stay Safe - and help to keep each other safe – when working online, be careful what personal information you give away about yourself and others, either as text or in a picture.

Be Responsible – take time to think about what you write, your intended audience and others who might be able to read it. You are in control of your actions. We are a caring school – look after each other, report anything you feel uncomfortable about or any unfair comments you see to a responsible adult.

Be Respectful – Look after each other, don't give away personal information or use images of other people without their permission. If the tools you use allow you to leave a comment and you have nothing constructive to say, then don't say anything at all.

_____

I agree to use the tools in BGFL 365 appropriately and will do my best to **stay safe, be responsible and be a respectful user.** I will do my best to help make the Internet a safe place to be.

Signed: ………………………………………. Class ……………… Date: …………………………..

Note to Parents: BGfL 365 is a great environment for schools to deliver the curriculum in a modern, creative way. It offers a fantastic range of digital tools to engage learners and meet the needs of the computing curriculum. Please take time to talk to your child and do a recap on the information above. All of the work your child creates using BGfL 365 sits on servers inside the EU and is covered by the data protection regulations.