Ss. Peter & Paul Catholic Primary School

E-Safety Policy

September 2020

This policy was fully adopted by the Governing Body on:

This policy will be reviewed on:

Last updated: September 2020

Contents:

Last updated: September 2020

Statement of intent

At Ss. Peter & Paul School 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.

Whilst the school recognises 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.

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, Child Protection and Safeguarding Policy and Allegations Against Staff Policy.

Signed by:

________________________ Headteacher Date: ____________________________

________________________ Chair of governors Date: ____________________________

Last updated: September 2020

1. Legal framework

1.1. This policy has due regard to the following legislation, including, but not limited to:

- The Human Rights Act 1998
- The Data Protection Act 1998
- The Safeguarding Vulnerable Groups Act 2006
- The Education and Inspection Act 2006
- The Computer Misuse Act 1990, amended by the Police and Justice Act 2006

2. Use of the internet

2.1. The understanding 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. Roles and 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, **Mrs Graham**, is responsible for ensuring the day-to-day e-safety in our school and managing any issues.

3.3. The headteacher 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.

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

3.5. The headteacher 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.

3.6. The e-safety officer will regularly monitor the provision of e-safety in the school and return this to the headteacher.

3.7. The school will establish a procedure for reporting incidents and inappropriate internet use, either by pupils or staff.

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

3.9. The e-safety officer will 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.

3.10. The governing body will hold regular meetings with the headteacher and/or e-safety officer to discuss the effectiveness of the e-safety provision, current issues, and to review incident logs.

3.11. The governing body will evaluate and review this E-safety Policy on an annual basis.

3.12. The headteacher 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.

3.13. Teachers are responsible for ensuring that e-safety issues are embedded in the curriculum and safe internet access is promoted at all times.

3.14. All staff are responsible for ensuring they are up-to-date with current e-safety issues, and this E-safety Policy.

3.15. All staff and pupils will ensure they understand and adhere to the **Acceptable Use Policy,** which they must sign and return to the headteacher.

3.16. Parents/carers are responsible for ensuring their child understands how to use computer technology and other digital devices, appropriately.

3.17. The headteacher is responsible for communicating with parents regularly and updating them on current e-safety issues and control measures.

4. 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 regular 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 Policy.**
- A record will be kept by the headteacher of all pupils who have been granted internet access.
- 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 headteacher.
- 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 headteacher for regular monitoring of activity.

4.4. Email:

- Pupils and staff will be given approved email accounts and are only able to use these accounts.
- Use of personal email 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 headteacher.
- Pupils are regularly educated on the implications of posting personal data online, outside of the [school/academy].
- Staff are regularly educated on posting inappropriate photos or information online, which may potentially affect their position and the school as a whole.

  Staff are not permitted to communicate with pupils over social networking sites and should use their professional judgement when adding parents. If unsure, please seek advice from the headteacher (updated 12.3.18).

4.6. Published content on the school website and images:

- The headteacher 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 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 headteacher 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.

5. Cyber bullying

5.1. 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.

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

5.3. 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.

5.4. 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.

5.5. 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.

5.6. The headteacher will decide whether it is appropriate to notify the police or anti-social behaviour coordinator in their LA of the action taken against a pupil.

6. Reporting misuse

6.1. Misuse by pupils:

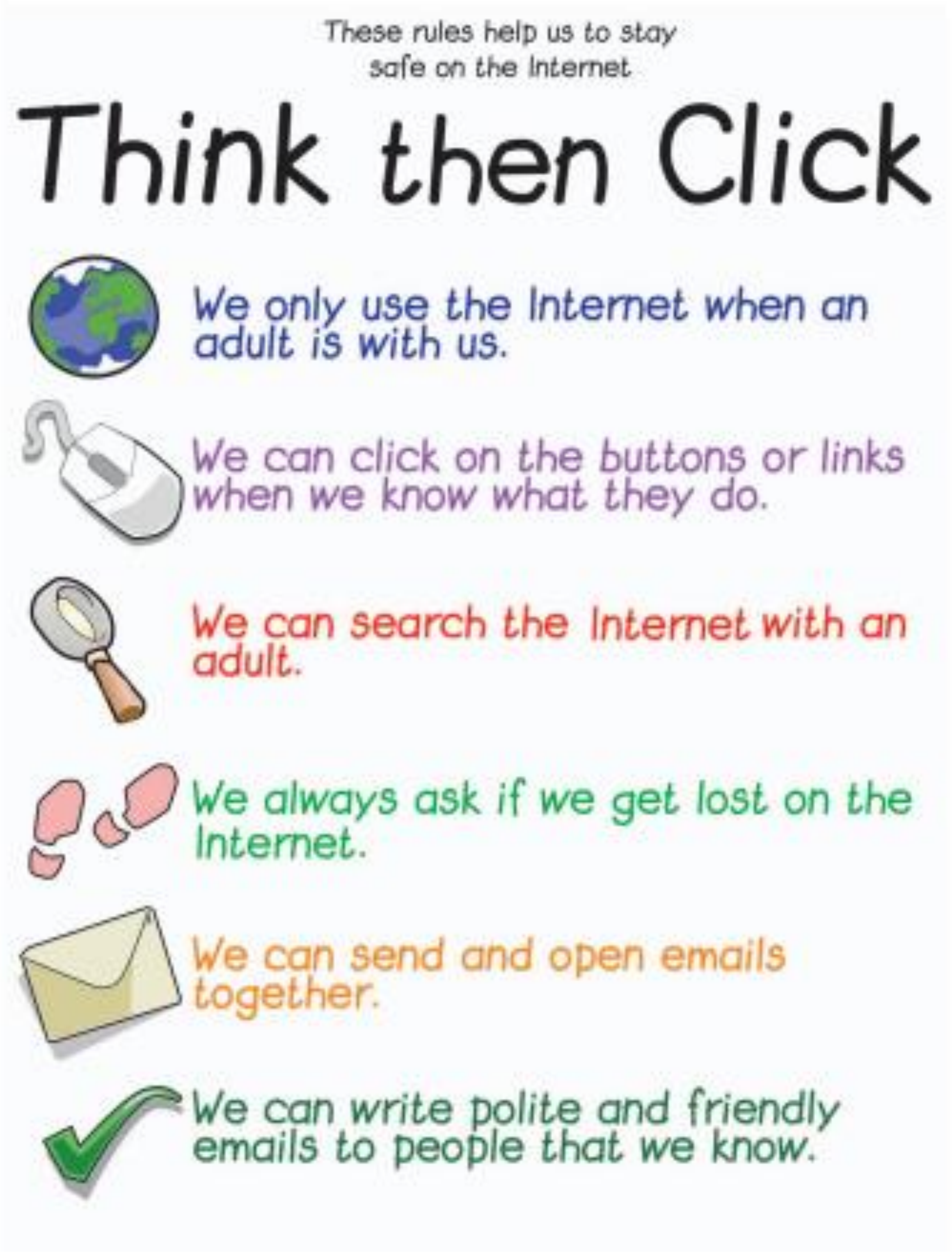
- Teachers have the power to discipline pupils who engage in misbehaviour with regards to internet use.
- Any instances of misuse should be immediately reported to a member of staff, who will then report this to the headteacher, using a complaints form.
- Any pupil who does not adhere to the rules outlined in our **Acceptable Use 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 headteacher and will be issued once the pupil is on the school premises.
- Complaints of a child protection nature shall be dealt with in accordance with our Child Protection Policy.

6.2. Misuse by staff:

- Any misuse of the internet by a member of staff should be immediately reported to the headteacher, using a complaints form.
- The headteacher will deal with such incidents in accordance with the Allegations Against Staff Policy, and may decide to take disciplinary action against the member of staff.
- The headteacher will decide whether it is appropriate to notify the police or anti-social behaviour coordinator in their LA of the action taken against a member of staff.

Appendices

E-Safety Rules for KS1



These rules help us to stay safe on the Internet

Think then Click

We only use the Internet when an adult is with us.

We can click on the buttons or links when we know what they do.

We can search the Internet with an adult.

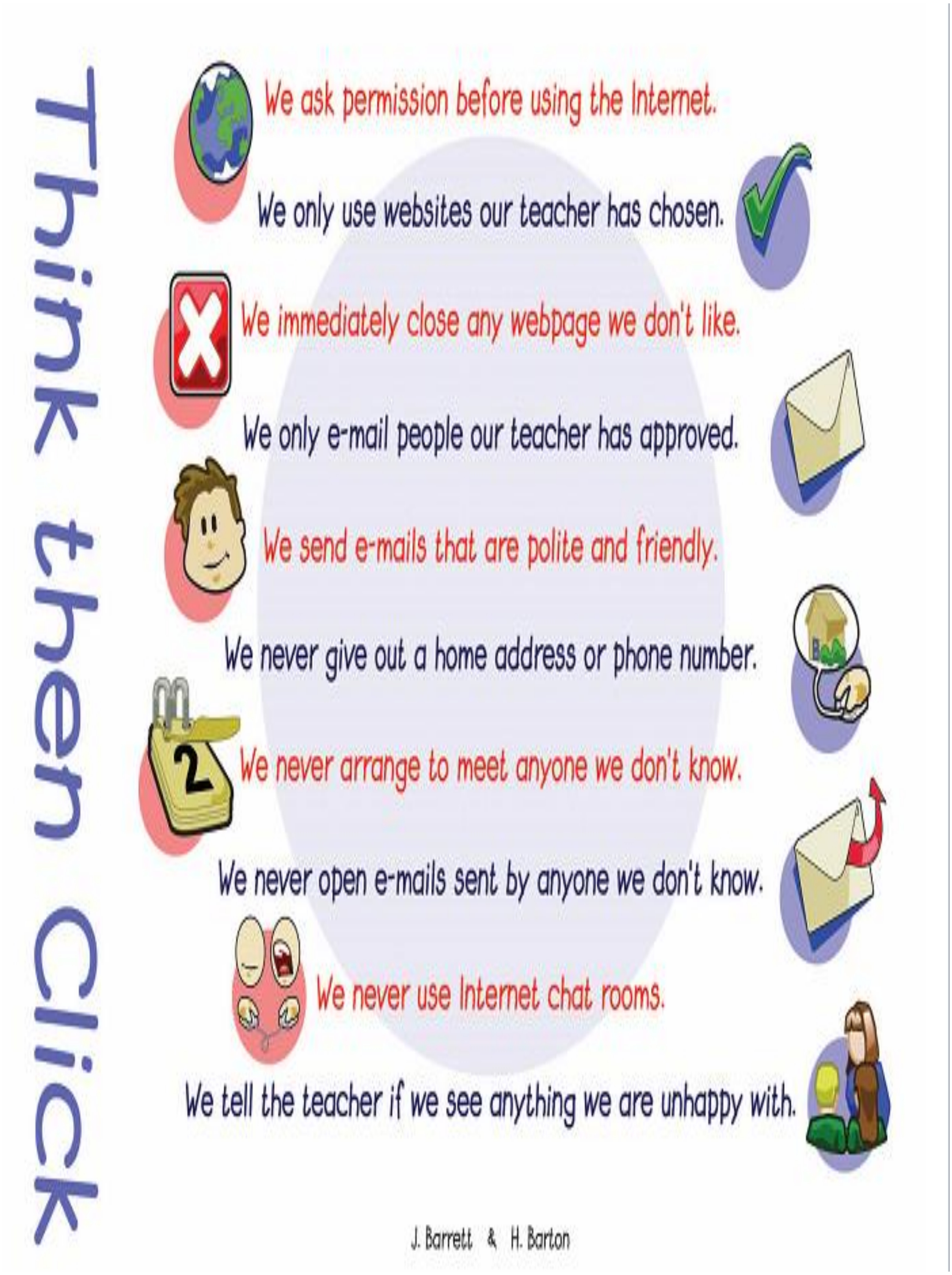
We always ask if we get lost on the Internet.

We can send and open emails together.

We can write polite and friendly emails to people that we know.

E-Safety Rules for KS2

Last updated: September 2020



Think then Click

We ask permission before using the Internet.

We only use websites our teacher has chosen.

We immediately close any webpage we don't like.

We only e-mail people our teacher has approved.

We send e-mails that are polite and friendly.

We never give out a home address or phone number.

We never arrange to meet anyone we don't know.

We never open e-mails sent by anyone we don't know.

We never use Internet chat rooms.

We tell the teacher if we see anything we are unhappy with.

J. Barrett & H. Barton

Agreement/E-safety rules

- I will use ICT in school only for studying purposes.
- When e-mailing, I will use my class or school e-mail address.
- I will not share my ICT passwords.
- I will only delete or open my own files.
- I will only open e-mail attachments from people known to me or people who my teachers have approved.
- I will make sure ICT communication with other pupils and adults is polite and responsible.
- I will not send pupils or adults any content which is unpleasant. If I find something like this, I will report it to my teacher.
- I will not share details of my name, phone number or address.
- I will not meet someone unless it is part of a school project and/or a responsible adult is present with me.
- I am responsible for my behaviour while using ICT.
- I will not upload images, sound, video or text content that could upset pupils, staff and others.
- I know that my use of ICT can be checked and that my parent/carer will be contacted if a member of school staff is concerned about my e-safety.
- If I see something online that makes me feel uncomfortable, I will inform my class teacher.

Ss Peter & Paul Catholic Primary School

Atherton Street, Wallasey, Wirral, CH45 9LT

Tel: 0151 639 2991 Fax: 0151 638 5232

schooloffice@stpeter-stpauls.wirral.sch.uk

Dear Parents & Carers,

The use of ICT including the internet, e-mail, mobile, social networking etc. has become a crucial part of learning and we want all pupils to be safe and responsible while using these valuable resources.

Please 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 school.

Yours sincerely,

Mrs P. Graham
(Headteacher)

✂ -

Parent/carer signature

We have discussed this and

……………………………………......... (child's name) agrees to follow the e-safety rules and to support the safe use of ICT at Ss. Peter & Paul School.

Parent/Carer signature

…………………………………………………………………

Child's class ………………………. Date ………………………………

Last updated: September 2020

Staff (and Volunteer) Acceptable Use Policy Agreement

1.1 School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools / academies and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

1.1.1.1 This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that staff and volunteers will have access to digital technology to enhance their work, to enhance learning opportunities for learning and will, in return, expect staff and volunteers to agree to be responsible users.

1.2 Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that learners receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

1.2.1.1 For my professional and personal safety:

- I understand that the school will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, VLE etc.) out of school, and to the transfer of personal data (digital or paper based) out of school
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school. (Please refer to overleaf sections 1.2 to 1.5 which relate to the personal use, by staff and volunteers, of school systems) (updated 12.3.18)

- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

1.2.1.2 I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (eg on the school website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites in school in accordance with the school's policies (for instance the school Twitter account).
- I will only communicate with learners and parents / carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

1.2.1.3 The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my mobile devices (laptops / tablets / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the school ICT systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted , or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try

to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.

- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School / LA Personal Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.
- I understand that data protection policy requires that any staff or student / pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

1.2.1.4 When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

1.2.1.5 I understand that I am responsible for my actions in and out of the school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could a warning, a suspension, referral to Governors / Directors and / or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name: ....

Signed: ....

Date: ....

Last updated: September 2020