St Edward's Catholic Junior School

"I can do all things through Christ who strengthens me."
Philippians 4:13

Policy for
Acceptable Use of ICT and E-safety

June 2019

This policy was adopted: June 2019

The policy is to be reviewed: June 2020

Contents

1. Introduction

ICT is as an essential resource to support learning and teaching, as well as playing an important role in our everyday lives. A sound foundation in ICT/computing in primary school will give children the skills to access life-long learning and employment.

At the moment, internet technologies children and young people are using both inside and outside of the classroom include websites, E-mail, instant messaging, tablets and mobile phones. It is important to recognise the constant and fast paced evolution of ICT/computing.

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these internet technologies.

At St Edward's Catholic Junior School, we understand the responsibility to educate our pupils on E-safety issues; teaching them the appropriate behaviours and skills to enable them to remain both safe and legal when using ICT, both inside and outside the classroom.

Both this policy and the Acceptable Use Agreement (see appendices 3 and 4) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, iPads, digital cameras, whiteboards, etc) and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones, camera phones, etc).

2. Roles and Responsibilities

The Head Teacher and Governors have ultimate responsibility to ensure that the E-safety Policy is monitored.

Our E-safety co-ordinator is: **Gemma Moncada / Randal Stokes**

All members of the school community have been made aware of who holds this post. It is the role of the E-safety co-ordinator to keep abreast of current issues and guidance through organisations such as Bucks LEA, Becta, CEOP (Child Exploitation and Online Protection) and Childnet.

Senior Management and Governors are kept informed by the E-safety co-ordinator. All Governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

This policy, supported by the school's Acceptable Use Agreements for staff, Governors, visitors and pupils, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: child protection, health and safety, behaviour, anti-bullying and PSHE policies and home-school agreements**.**

2.1 E-safety Skills: Development for Staff

- Regular training is provided by the E-safety coordinator to ensure staff are kept up to date
- New staff access a copy of the E-safety Policy, and sign the staff Acceptable Use Agreement, as part of their induction.
- All staff are aware of individual responsibilities relating to the safeguarding of children within the context of E-safety and know what to do in the event of misuse of technology by any member of the school community (see Appendix 1)
- All staff incorporate E-safety activities as part of the computing curriculum and raise awareness within other curriculum areas (e.g. PSHE, assemblies).

2.2 Designated safeguarding person

Should be trained in E-safety issues and be aware of the potential for serious child protection issues which may arise from:

- Sharing of personal data.
- Access to illegal or inappropriate materials.

- Inappropriate on-line contact with adults or strangers.
- Potential or actual incidents of grooming.
- Cyber-bullying.

2.3 Managing the school E-safety messages

- We endeavour to embed E-safety messages across the curriculum whenever the internet and/or related technologies are used.
- Each pupil will sign the pupils' Acceptable Use Agreement/E-safety Rules. Rules for safety will be discussed and reviewed by staff and pupils regularly
- E-safety posters will be prominently displayed.
- Our School Website informs pupils about E-safety and the implications of cyber-bullying.

3. Use of the Internet

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. All use of the **internet and associated software (e.g. capita/e-schools etc)** is logged and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected it will be followed up.

3.1 Responsible use of the internet

- The school expects all users to use the internet responsibly.
- Users shall not: Visit Internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:
    - pornography (including child pornography)
    - promoting discrimination of any kind
    - promoting racial or religious hatred
    - promoting illegal acts
    - any other information which may be offensive to colleagues
- Students will have supervised access to Internet resources (where reasonable) through the school's internet technology.
- Staff will preview any recommended sites before use and where necessary will advise pupils on how to create safe usernames and passwords, use online sites responsibly and seek parental permission for use of online services e.g. google, scratch, survey monkey etc.
- When researching using search engines pupils will be supervised and will be taught to search responsibly and will know what to do if inappropriate material appears. They will have an understanding of how to use reliable sources.
- If Internet research is set for homework, parents will be advised to supervise research.
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.
- All users must observe copyright of materials from electronic resources.
- Staff and pupils should not download software, media or files without first seeking authorisation.
- If inappropriate material is accessed accidentally it should be reported to the Head Teacher or E-safety co-ordinator so appropriate action can be taken.

3.2 Internet Games

There are times when children have 'free' use of the school network, such as during computer clubs, reward time for good behaviour etc. Any games played on the school network must be in line with the school Code of Conduct and be suitable for primary aged children.

3.3 Monitoring

- St Edward's has a monitoring solution where web-based activity is monitored and recorded.
- School internet access is controlled through a web filtering service. Staff may request blocked sites to be made available if they contain information relevant to their subjects. Requests should be made to the service provider.

- St Edward's Catholic Junior School is aware of its responsibility when monitoring staff communication under current legislation and takes into account; Data Protection Act 1998, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998, Computer Misuse Act 1990.
- Staff and pupils are aware that school based e-mail and internet activity can be monitored and explored further if required.
- The school does not allow pupils access to internet logs.
- If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the E-safety co-ordinator.
- It is the responsibility of the school, by delegation to the network manager, to ensure that Anti-virus protection is installed and kept up-to-date on all school machines.
- If there are any issues related to viruses or anti-virus software, the network manager should be informed.

4. Data Protection and System Security

4.1 Password security

- Password security is essential for staff, particularly as they are able to access and use pupil data. Members of staff are expected to have secure passwords which are not shared with anyone or written down anywhere. Staff and pupils are regularly reminded of the need for password security.
- Staff should never let pupils logon with their username and password and all children have individual user names and passwords for the network.
- If users think their passwords have been misused, or their logon details are not working they must report this to Mrs G Moncada or TurnitOn
- Pupils are not allowed to deliberately access files on the school network belonging to their peers, teachers or others.
- Individual staff users must make sure that unattended workstations are locked.

4.2 System and Data Security

- Staff are aware of their responsibility when accessing school data. Level of access is determined by the Head Teacher.
- Data can only be accessed and used on school computers or laptops. Staff are aware they must not use their personal devices for accessing any school/ children/ pupil data.
- The school laptop should not be shared with any unauthorised person.
- Equipment is more vulnerable once it leaves the building. Laptops, mobile technology and pen drives are susceptible to theft and loss along with its data. All data should be saved to the server where possible as opposed to portable devices and pen drives.
- Data should be backed up by the server provider.

5. Mobile technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning. Many existing mobile technologies such as portable media players, gaming devices, tablets and Smart phones are familiar to children outside of school, thus opening up the risk and misuse associated with communication and internet use.

5.1 Personal Mobile devices (including phones)

- The school allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the school allow a member of staff to contact a pupil or parent/ carer using their personal device. This will apply for 5 years following the pupil leaving the school, unless the members of staff know the family personally.
- Pupils are allowed to bring personal mobile devices/phones to school but must not use them for personal purposes within lesson time. They must be handed into the office at the start of the day.

- This technology may be used, however, for educational purposes, as mutually agreed with the Head Teacher. The device user, in this instance, must always ask the prior permission of the bill payer.
- The school is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate text messages between any member of the school community is not allowed.
- Permission must be sought before any image or sound recordings are made on these devices of any member of the school community.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

5.2 School provided Mobile devices (including phones, iPads and Netbooks)

- The sending of inappropriate text messages between any member of the school community is not allowed.
- Permission must be sought before any image or sound recordings are made on the devices of any member of the school community. This is done as part of the signed Acceptable Use Agreements (appendices 3, 4 and 5)
- Where the school provides mobile technologies such as phones, laptops and iPads for offsite visits and trips, only these devices should be used.

6. E-mail

The use of e-mail is an essential means of communication. In the context of school, e-mail should not be considered private. Educationally, e-mail can offer significant benefits including: direct written contact between schools on different projects (staff or pupils), within school, or internationally. We recognise that pupils need to understand how to style an e-mail in relation to their age and good 'netiquette' (network etiquette).

- The school gives all staff their own e-mail account to use for all school business. This is to minimise the risk of receiving unsolicited or malicious e-mails and avoids the risk of personal profile information being revealed.
- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary e-mail histories can be traced. This should be the account that is used for all school business.
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal e-mail addresses.
- E-mail sent to an external organisation should be written carefully before sending, in the same way as a letter written on school headed paper.
- Staff sending e-mails to parents are advised to copy (cc) the Head Teacher or line manager.
- Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes.
- All children are able to access their own individual school issued accounts via google.
- The forwarding of chain letters is not permitted in school. Pupils and staff who receive chain letters should forward any chain letters to the E-safety co-ordinator immediately.
- All e-mail users are expected to adhere to the generally accepted rules of netiquette particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Pupils must immediately tell a teacher/ trusted adult if they receive an offensive e-mail.
- Staff must inform the E-safety co-ordinator if they receive an offensive e-mail.
- Pupils are introduced to e-mail as part of the computing curriculum. By the time they leave Year 6, they will have experienced sending and receiving e-mails.
- Pupils are made aware that they must not open or reply to e-mails from people they don't know, as this compromises their security.

7. Digital Media

7.1 Taking of Images and Film

Digital images are easy to capture, reproduce and publish and are often misused. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.

- With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images and videos by staff and pupils with school equipment.
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images or videos of pupils, this includes when on field trips. However, with the express permission of the Head Teacher, images can be taken provided they are transferred immediately and solely to the schools network and deleted from the staff device.
- Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images or videos of the others, this includes when on field trips.

7.2 Consent of adults who work at the school

Permission to use images and videos of all staff who work at the school is sought on induction and a copy is located in the personnel file

7.2 Publishing pupil's images and work

On a child's entry to the school, all parents/guardians will be asked to give permission to use their child's work/photos in the following ways:

- on the school web site
- in the school prospectus and other printed publications that the school may produce for promotional purposes
- recorded/ transmitted on a video or webcam
- in display material that may be used in the school's communal areas
- in display material that may be used in external areas, ie exhibition promoting the school
- general media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically).

- This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, e.g. divorce of parents, custody issues, etc.
- Parents/ carers may withdraw permission, in writing, at any time.
- Pupils' names will not be published alongside their image and vice versa. E-mail and postal addresses of pupils will not be published. Pupils' full names will not be published.
- Before posting student work on the Internet, a check will be made to ensure that permission has been given for work to be displayed.

7.3 Storage of Images

- Images/ films of children are stored on the school's network.
- Pupils and staff are not permitted to use personal portable media for storage of images (e.g., USB sticks) without the express permission of the Head Teacher.
- Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network and Waddle.

7.4 Webcams and CCTV

- We do not use publicly accessible webcams in school.
- Webcams in school are only ever used for specific learning purposes, i.e. monitoring hens' eggs and never use images of children or adults.
- Misuse of the webcam by any member of the school community will result in sanctions (as listed under the 'inappropriate materials' section of this document).

7.5 Video Conferencing

- Permission is sought from parents and carers if their children are involved in video conferences
- Permission is sought from parents and carers if their children are involved in video conferences with end-points outside of the school.
- All pupils are supervised by a member of staff when video conferencing.
- All pupils are supervised by a member of staff when video conferencing with end-points beyond the school.
- The school keeps a record of video conferences, including date, time and participants.
- Approval from the Head Teacher is sought prior to all video conferences within school.
- The school conferencing equipment is not set to auto-answer and is only switched on for scheduled and approved conferences.
- No part of any video conference is recorded in any medium without the written consent of those taking part.

8. E-safety in the Curriculum

- The school has a framework for teaching about E-safety in computing lessons through the computing curriculum.
- The school provides opportunities within a range of curriculum areas (e.g. computing, PSHE, assemblies, drama) to teach about E-safety, and dangers that may arise both inside and outside of school.
- Pupils are taught to respect other people's information, images, etc through discussion, modelling and activities. Older pupils are taught about copyright.
- Pupils are aware of the impact of online bullying and know how to seek help if they are affected by these issues.
- Pupils are aware of where to seek advice or help if they experience problems when using the internet and related technologies (e.g. access to unsuitable material) Sources of help may be: parent/ carer, teacher/ staff member, an organisation such as Childline/ CEOP report abuse button, etc.
- Pupils are taught to learn good searching skills through cross curricular teacher models, discussions and via the computing curriculum.
- Pupils are taught to be critical of sources and recognise reliable sources.

9. Misuse and Infringements

9.1 Complaints

Complaints relating to E-safety should be made to the E-safety co-ordinator or Head Teacher. Incidents should be logged and the **Buckinghamshire Flowcharts for Managing an E-safety Incident** should be followed (see appendix 1).

9.2 Inappropriate material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the E-safety co-ordinator.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the E-safety co-ordinator, depending on the seriousness of the offence (see appendix 1).
- Users are made aware of sanctions relating to the misuse or misconduct through the Pupils' Acceptable User Agreement.

10. Equal Opportunities

Pupils with additional needs

The school endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the schools' E-safety rules.

However, staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of E-safety issues.

Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of E-safety. Internet activities are planned and well managed for these children and young people.

11. School Website

Any work published on the school website is thoroughly checked to ensure that there is no content that compromises the safety of pupils or staff. The content of the website should be of a high quality and will be regularly updated to ensure that it reflects the school accurately.

12. Parental Involvement

We believe that it is essential for parents/ carers to be fully involved with promoting E-safety both in and outside of school. We regularly consult and discuss E-safety with parents/ carers and seek to promote a wide understanding of the benefits related to ICT and associated risks.

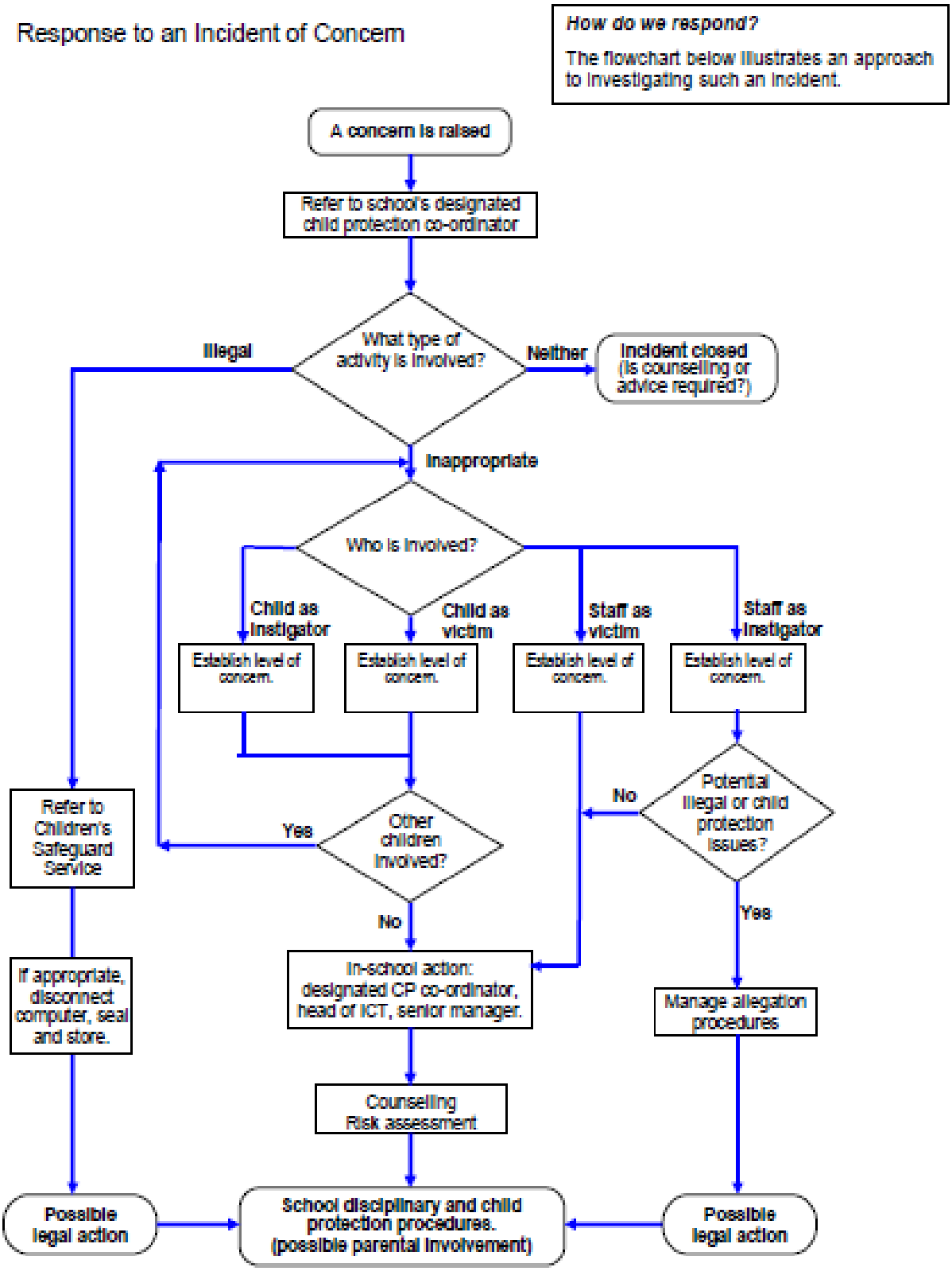
- Parents/ carers and pupils are actively encouraged to contribute to adjustments or reviews of the school E-safety policy by e-mailing suggestions to the school office.
- Parents/ carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to school.
- Parents/ carers are required to sign a form as to whether or not they consent to images of their child being taken/ used in the public domain (e.g., on school website).
- The school disseminates information to parents relating to E-safety where appropriate in the form of;
    - Information evenings
    - Posters
    - Links to websites
    - Newsletter items

13. Writing and Reviewing this Policy

There will be an on-going opportunity for staff to discuss any issue of E-safety that concerns them.
They can bring their concerns to the attention of the E-safety co-ordinator at any time. This policy will be reviewed every (12) months and consideration given to the implications for future whole school development planning. The policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way.

This policy has been read, amended and approved by the staff, Head Teacher and Governors.

Appendix 1 - Buckinghamshire Flow Chart
Response to an E-safety incident



Appendix 2

Acceptable Use Agreement
Staff, Governors and Visitors

ICT and the related technologies such as e-mail, 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 members of staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with Mrs Gemma Moncada, School E-safety Co-ordinator.

- I will only use the school's e-mail / Internet / Intranet and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- 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 communicate with any pupils using personal mobile technology, within 5 years of them leaving the school.
- I will not give out my own personal details, such as mobile phone number and personal e-mail address, to pupils.
- I will only use the approved, secure e-mail system for any school business.
- I will ensure that personal data (such as data held on SIMS) 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 Head or Governing Body.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- I will not purchase or download APPS onto school technologies (i.e. iPads) without seeking authorisation
- 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 Head Teacher.
- 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 Head Teacher.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's E-safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.

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

Full Name (Printed) ……

Signature …… Date …….

Job Title ……

Appendix 3

Primary Pupil Acceptable Use Agreement / E-safety Rules

RESPONSIBILITIES

- ✓ I will be responsible for my behaviour when using ICT.
- ✓ I will only use ICT in school for school purposes.
- ✓ I will only open/delete my own files.
- ✓ I will not take a camera on any school trips or residentials.
- ✓ I will not deliberately look for, save or send anything that could be unpleasant or nasty.
- ✓ I will follow the SMART rules

S – SAFE

- ✓ I will not tell other people my passwords or ask other people for theirs.
- ✓ I will not give out my own details such as my name, phone number or home address.
- ✓ I will not upload photos or videos of anyone at school to the internet.

M – MESSAGING AND MEETING

- ✓ I will only use my own school e-mail address when e-mailing.
- ✓ I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- ✓ I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.

A - ACCEPTING

- ✓ I will only open e-mail attachments from people I know, or who my teacher has approved.
- ✓ I will not talk to people I do not know when using the internet

R- RELIABLE

- ✓ I will think carefully about the information on the internet

T - TELL

- ✓ If I accidentally find anything that is unpleasant or nasty I will tell my teacher immediately.
- ✓ If I receive anything that makes me feel uncomfortable I will tell my teacher or an adult I trust immediately

MONITORING

- ✓ I know that my use of ICT can be checked and that my parent/ carer contacted if a member of school staff is concerned about my E-safety.
- ✓ I understand that if break **any** of the rules in this Agreement, my parents will be informed and I will be banned from using the internet at school.

Pupil Name ……..

Class …….

Signature …… Date ……..

Appendix 4

Parents/Carers Agreement

Internet and ICT: As the parent or legal guardian of the pupil(s) named below, I grant permission for the school to give my daughter/son access to:

- The Internet at school
- The school's chosen e-mail system
- The school's online managed learning environment
- ICT facilities and equipment at the school

I accept that ultimately the school cannot be held responsible for the nature and content of the materials accessed through the Internet and mobile technologies, but I understand that the school takes every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials.

I understand that the school can, if necessary, check my child's computer files and the Internet sites they visit at school, and if there are concerns about my child's E-safety or e-behaviour they will contact me.

Use of digital images, photography and video: I understand the school has a clear policy on "The use of digital images and video" and I support this.

I understand that the school will use photographs or videos of my child to support learning activities.

I accept that the school may use photographs/videos that include my child in publicity that reasonably promotes the work of the school, and for no other purpose.

I will not share photographs of other children (or staff) at school events without permission.

Social networking and media sites: I understand that the school has a clear protocol for "The use of social networking and on-line media" (Appendix 6) and I support this.

I understand that the school takes any inappropriate behaviour seriously and will respond to observed or reported inappropriate or unsafe behaviour.

I will support the school by promoting safe use of the Internet and digital technology at home. I will inform the school if I have any concerns.

My Child's Name ……..

Parent/Carer Signature ……..

Class …… Date ……..

Class …… Date ……

If you have any queries or concerns, please contact the school office or your child's class teacher.

This form is valid for five years from the date you sign it, or for the period in which your child attends this school.

Alternative Parents/Carers Agreement
(to be provided upon request)

Internet and ICT: As the parent or legal guardian of the pupil(s) named below, I grant permission for the school to give my daughter/son access to:

- The Internet at school
- The school's chosen e-mail system
- The school's online managed learning environment
- ICT facilities and equipment at the school

I accept that ultimately the school cannot be held responsible for the nature and content of the materials accessed through the Internet and mobile technologies, but I understand that the school takes every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials.

I understand that the school can, if necessary, check my child's computer files and the Internet sites they visit at school and if there at school and if there are concerns about my child's E-safety or e-behaviour they will contact me.

Use of digital images, photography and video: I understand the school has a clear policy on "The use of digital images and video" and I support this.

I understand that the school will use photographs or videos of my child to support learning activities.

I will not share photographs of other children (or staff) at school events without permission.

Social networking and media sites: I understand that the school has a clear protocol for "The use of social networking and on-line media" sites and I support this.

I understand that the school takes any inappropriate behaviour seriously and will respond to observed or reported inappropriate or unsafe behaviour.

I will support the school by promoting safe use of the Internet and digital technology at home. I will inform the school if I have any concerns.

My Child's Name ……

Class …… Date ……

Parent/Carer Signature ……

This form is valid for five years from the date you sign it, or for the period in which your child attends this school.

Appendix 5

Protocol on The use of digital images and video

To comply with the Data Protection Act 1998, we need your permission before we can photograph or make recordings of your daughter/son.

We follow the following rules for any external use of digital images:

If the pupil is named, we avoid using their photograph.
If their photograph is used, we avoid naming pupil.

Where showcasing examples of pupils work we only use their first names, rather than their full names or give any personal details e.g. e-mail or postal addresses or telephone numbers.

If showcasing digital video work to an external audience, we take care to ensure that pupils aren't referred to by name on the video, and that pupils' full names aren't given in credits at the end of the film.

Only images of pupils in suitable dress are used.

Staff are not allowed to take photographs or videos on their personal equipment.

Examples of how digital photography and video may be used at school include:

- Your child being photographs (by the class teacher or teaching assistant) as part of a learning activity e.g. taking photos or a video of pupils' with their artwork
- Your child's image being used for presentation purposes around the school; e.g. in class or wider school wall displays
- Your child's image being used in a presentation about the school and its work in order to share their good practice and celebrate their achievements, which is shown to other parents, schools or educators e.g. within our school prospectus or on the website.

Note: If we, or you, actually wanted your child's image linked to their name we would contact you separately for permission e.g. if your child was at a public event and wanted to be names in local literature i.e. newspaper.

Appendix 6

St Edward's Catholic Junior School

"I can do all things through Christ who strengthens me".
Philippians 4: 13

The use of social networking and on-line media

This school asks its whole community to promote the 3 commons approach to online behaviour:

- **Common courtesy**
- **Common decency**
- **Common sense**

How do we show common courtesy online?

- We ask someone's permission before uploading photographs, videos or any other information about them online.
- We do not write or upload **'off-hand', hurtful, rude or derogatory comments and materials.** To do so is disrespectful and may upset, distress, bully or harass.

How do we show common decency online?

- We do not post comments that can be considered as being **intimidating, racist, sexist, homophobic or defamatory. This is cyber-bullying** and may be harassment or libel.
- When such comments exist online, we do not forward such emails, tweets, videos, etc. By creating or forwarding such materials we are all liable under the law.

How do we show common sense online?

- We think before we click.
- We think before we upload comments, photographs and videos.
- We think before we download or forward any materials.
- We think carefully about what information we share with others online, and we check where it is saved and check our privacy settings.
- We make sure we understand changes in use of any web sites we use.
- We block harassing communications and report any abuse.

Any actions online that impact on the school and can potentially lower the school's (or someone in the school) reputation in some way or are deemed as being inappropriate will be responded to.

In the event that any member of staff, student or parent/carer is found to be posting libellous or inflammatory comments on Facebook or other social network sites, they will be reported to the appropriate 'report abuse' section of the network site.

(All social network sites have clear rules about the content which can be posted on the site and they provide robust mechanisms to report contact or activity which breaches this.)

In serious cases we will also consider legal options to deal with any such misuse.

The whole school community is reminded of the CEOP report abuse process:

https://www.thinkuknow.co.uk/parents/browser-safety/