Edmund's Catholic Primary School

&

St Joseph's Catholic Primary School

ONLINE SAFETY POLICY

Policy Adopted: Autumn 2020

Reviewed: Autumn 23

Review Date: Autumn 24

Contents

Related Policies and associated documents:

This policy should be read in conjunction with the following policies:

- Child Protection and Safeguarding (online safeguarding areas including content, contact and conduct)
- Confidentiality agreement (GDPR and social media posting)
- Financial controls for staff (use of computers off site/insurance, installation of software)
- Data Protection Policy (GDPR personal data and images)
- Own Device Policy (use of personal devices in school)
- Behaviour and Discipline Policy (cyberbullying)
- Staff Handbook (teaching standards and expectations)
- Acceptable Use Policies

Introduction

Online Safety encompasses Internet technologies and electronic communications. It highlights the need to educate children about the benefits and risks of using new technologies and provides safeguards and awareness for users to enable them to control their online experiences.

Online Safety depends on effective practice at a number of levels:

- Responsible use of digital technologies by all staff and pupils; encouraged by education and made explicit through published policies.
- Sound implementation of the Online Safety policy in both administration and curriculum, including secure school infrastructure design and use.

The policy applies to all those accessing information and network services provided by the school including staff (including non-teaching staff), contractors, visitors, governors, parents and pupils.

Vision

At The Federation of St Edmund's and St Joseph's Catholic Primary Schools we value Computing and the use of technology inside and outside of the classroom. We recognise the impact technology has on the world around us and we understand the need to prepare our children to meet the technological environment within and beyond the school. Online Safety is an important part of our vision.

- We expect children to become confident, creative users of technology: Children will be expected to make decisions regarding their own use of technology, choosing varied and appropriate technologies to suit a purpose.
- Children will become independent risk takers, not being afraid to try new things and experiment with different technologies.
- Children will become question askers, developing analytical skills. They will learn to assess their own methods and use of technology.
- Children will be safe users of technology, understanding how to keep themselves safe through knowledge of the risks technology can pose.

In addition we are committed to the effective use of technology to support teaching, administration and communication within the school community.

Entitlement and Equal Opportunities

All should have equal access to appropriate digital technologies in order to develop their personal computing capability.

- The SENDCO will advise teachers on the digital technologies support that can be provided to individual pupils with particular education needs, including high ability pupils.
- We consider ways in which pupils with a computer at home can be encouraged to use it for educational benefit, particularly through the provision of online services such as Mathletics, Time Table RockStars and Spelling Shed.
- Each child will be entitled to a computing lesson and in addition to this, laptops and iPads are available to be used within other curriculum areas.
- In the Foundation Stage, children will have daily opportunities to fulfil the requirements of the Early Years Foundation Stage (EYFS).

Online Safety in the School Community

Managed System

The school has an appropriate filtering system in place to reduce the risk of children being exposed to inappropriate internet content. This system is administered and maintained by our internet provider, which is the Local Authority's preferred internet provider. Although, this minimises the risk, there is always a chance that inappropriate materials will get through the filtering system.

The school is aware that its level of filtering is higher than that which the children may experience outside school, particularly at home. Therefore, our aim as a school, is to educate the children in managing risk, rather than attempting to completely remove it.

Online Safety in the Curriculum

Online Safety should be a focus in all areas of the curriculum and staff should reinforce Online Safety messages across the curriculum. In accordance with the Government's '*Teaching online safety in school'* (June 2019), the Online Safety curriculum should be provided in the following ways:

- A planned Online Safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils should be helped to understand the pupil Acceptable Use Policy and be encouraged to adopt safe and responsible use both within and outside school
- Staff should act as good role models in their use of digital technologies the internet and mobile devices
- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Children will be taught to identify online risks at their appropriate level each year throughout their time in school. These risks can be grouped under 3 headings, relating to Online Content, Online Contact and Online Conduct.

Online Content	Online Contact	Online Conduct

being exposed to illegal, inappropriate or harmful material, for example, pornography, fake news, racist or radical and extremist views	being exposed to harmful online interaction with other users, for example, commercial advertising as well as adults posing as children or young adults	personal online behaviour that increases the likelihood of, or causes, harm, for example, making, sending and receiving explicit images, or online bullying

A Progressive Curriculum

The Federation teaches Online Safety following the guidance from '*Education for a Connected World'* 2018 and using the '*Be Internet Legends'* curriculum produced by Google.

The Federation uses the Rising Stars Switched On Computing materials as a basis for its computing curriculum. Opportunities for teaching about Online Safety are identified within each unit, and teachers are also encouraged to identify Online Safety opportunities within their cross-curricular planning.

As part of the induction week at the beginning of the academic year, all class teachers discuss Online Safety with the class, and each class creates its own set of Online Safety rules which are displayed in the classroom.

The Use of Digital and Video Images in School

Staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images.
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (provided this falls within the GDPR). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils / pupils in the digital / video images.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes with exception of the Senior Leadership Team.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website; by the School / Home agreement signed by parents at the beginning of the year.

- Pupil’s work can only be published with the permission of the pupil and parents or carers; this again is generally covered by the School / Home agreement signed by parents at the beginning of the year.

Data Protection

Please refer to the Data Protection Policies and other policies relating to GDPR. In addition:

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Store and access personal data only on secure, encrypted password protected devices.
- Ensure that the device is logged-off or locked when the computer is unattended.

When personal data is stored on any portable computer system, memory stick or any other removable media:

- the data must be encrypted and password protected
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete

Communications

When using communication technologies the school considers the following as good practice:

- The email service used by the school may be regarded as safe and secure. Users should be aware that email communications are monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and pupils or parents / carers (email, chat etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Pupils should be taught about Online Safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Social Media – Protecting Professional Identity

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.

- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School staff should ensure that:

- No reference should be made in private social media posts to pupils, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.
- Information shared should not in any way bring the school or individuals into disrepute.

Online Safety for Staff

Induction

All members of staff need to be aware of the possible misuses of on-line access and their responsibilities towards pupils. Wherever possible the school will use firewalled services to try to ensure that undesirable material is unavailable to pupils.

The school has a set of guidelines for Internet use by pupils. All staff are responsible for explaining the rules and their implications. However, unsupervised pupil use of digital technology resources is not permitted within the Federation. The Federation complies with all appropriate legislative requirements.

As well as internet safety, staff and children alike, need to be aware of the constant threat to the security of the system, through viruses and other means of attack.

Online Safety Training for Staff and Volunteers

It is essential that all staff receive Online Safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal Online Safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the Online Safety training needs of all staff will be carried out regularly.
- The Online Safety leader will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- The Online Safety leader (or other nominated person) will provide advice / guidance / training to individuals as required.

Online Safety Training for Governors

Governors should take part in Online Safety training / awareness sessions, with particular importance for those who are members of any sub committee / group involved in technology / Online Safety / health and safety / child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association / or other relevant organisation.
- Participation in school training / information sessions for staff or parents (this may include attendance at assemblies / lessons).

Acceptable Usage Policy

All users of the school's online systems must sign the Acceptable Usage Policy relevant to their status. The possible statuses are:

- Early Years and Key Stage One Pupils
- Key Stage 2 Pupils
- Adults working with children; including governors, teachers, support staff, etc.
- Third Party, including visitors, contractors, etc.

Network Security

Any software, or files originating from outside of the school, including flash drives and memory keys, must be virus checked first before being opened or installed on the network.

The use of USB storage and other portable storage devices is prohibited by pupils on the school's computer network. Children should ask a member of staff to check and transfer any files necessary.

Staff should not generally use USB storage, but should store files in their personal documents area, the shared network drives or SharePoint. All of these areas are encrypted and backed up ensuring the security of the data. However if USB pens and portable devices are used, the member of staff is responsible for ensuring that these are virus free and encrypted (if containing personal data).

Staff, and pupils, should be aware of the importance of only accessing authentic and reliable websites. Many other sites contain malware, adware or other undesirable programmes which could affect the integrity and reliability of the computers and network. Generally, our virus protection software contains the ability to assess the risk of accessing various websites. Where a website is identified by the software as being at risk, that website must not be accessed.

All virus software must be updated on at least a twice-weekly basis to reduce the risk of infection. Where an infection is found (or identified by outside provider), that machine will be disconnected from the network until the infection has been cleaned.

School computers have their Windows Updates managed centrally, however if there are any technical problems with these updates the member of staff must return their laptop to the IT team to ensure updates are installed and the integrity of the network is maintained.

All users must be aware that only software authorised by the school, and for which the school holds a licence, may be installed on the computers. Additionally, no additional toolbars, e.g. Google, Yahoo, etc., apart from that provided by the security software may be installed on the computers.

All emails must also be scanned for viruses, and both staff and children made aware, that email attachments and pop-up buttons must never be opened unless 100% certain of the contents and origin of the file.

Children from Year 3 upwards have internal email accounts. All communications must be in connection with tasks set within school, no personal communications are allowed. Emails may be monitored to ensure that this is complied with.

The National Curriculum requires that pupils are taught about email and, to achieve this, the school teaches email through secure software; the children being unable to send emails out of, or receive emails from outside the school.

To account for possible changes in the future the following provisions are also included within this acceptable usage policy.

- Pupils may only use approved email accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive email.
- Pupils must not reveal personal details about themselves or others in email communication, or arrange to meet anyone without specific permission
- Whole class or group email addresses should be used in school
- Pupils may only use school email for classroom supported activities; the use of school email for other purposes is not permitted.
- Incoming email should be treated as suspicious and attachments not opened unless the author is known.
- Access in school to external personal email accounts may be blocked.
- Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.

Authorised Internet Access

The school will maintain a current record of all staff and pupils who are granted Internet access.

- All users must read and sign the 'Acceptable Use Policy' before using any school resource.
- Parents will be informed that pupils will be provided with supervised Internet access on school premises.
- Parents will be asked to sign and return a consent form for pupil access.
- Pupils will be asked to sign the Acceptable Usage Policy to accept the terms and conditions contained therein. This will be done on entry to the school and annually, either in written or digital form.
- The school's wireless internet system must be protected with a secure-encrypted key to prevent unauthorised access to the internet either from inside the school site or anywhere within range of the wireless signal.
- Only digital technology equipment owned by the school can be configured to access the internet using the school's network. Visitors may access the guest wifi with a temporary password.

Copyright, Intellectual Property and Plagarism

- All users of the school's digital technologies, should ensure that anything they post online is their own work and intellectual property.
- The only exceptions to the above rule is where materials have been identified as 'copyright free'; even in this case though, appropriate reference needs to be made to the source of the materials. Guidance on this is often on the web site the children are acquiring the information on.

Monitoring of Online Safety

How we monitor online safety:

- As part of the curriculum, all children will be taught how to report Online Safety concerns, both inside school and outside school
- Reporting and Recording of Online Safety Incidences
- All Online Safety incidences will be monitored by the school's Online Safety lead, who will use the Suffolk 'Incident Screening Tool and Reporting Guidance' – Online Safety and Cyberbullying Screening tool to identify the level of the incident and follow the appropriate procedure.
- Copies of all incidences are recorded in the Online Safety log which is stored in the school office.
- The impact of training events, both for parents and staff, will be monitored periodically to ensure that they are effective and fulfilling currently legislation and perceived need.

Cyberbullying

Cyberbullying can take a wide range of forms, including email, text or instant messaging, comments left on blogs and forums, etc.

As with all instances of bullying, cyber-bullying will be dealt with in accordance with the schools Behaviour and Discipline policy. In addition, there is the possibility that personal accounts could be suspended while incidents are being investigated.

If an individual (staff / pupil or parent) sees, or is emailed, something that upsets them, they can report it using the CEOP Report button at the bottom of the school's website home page. Alternatively the Online Safety Leader should be contacted.

Responding to Incidents of Misuse

There may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by children and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)

Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:

- Internal response or discipline procedures
- Involvement by Local Authority or national / local organisation (as relevant).
- Police involvement and/or action

If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:

- incidents of 'grooming' behaviour
- the sending of obscene materials to a child
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

Breach of Online Safety Guidelines

Where it is evident that the guidelines of the Online Safety policy are not being followed, the child or adult concerned will be spoken to and depending upon the seriousness of the breach, appropriate action taken and in the case of children, parents informed.

In extreme cases, that individual's access to the use of digital technologies within school can be suspended.

In the event of illegal activity taking place, external bodies including the police can be informed.

Responsibilities

Governors

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about Online Safety incidents and monitoring reports, as part of the school's safeguarding procedures

Head Teacher

- The Headteacher has a duty of care for ensuring the safety (including Online Safety) of members of the school community
- The Headteacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious Online Safety allegation being made against a member of staff.
- The Headteacher is responsible for ensuring that the Online Safety leader and other relevant staff receive suitable training to enable them to carry out their Online Safety roles and to train other colleagues, as relevant.
- The Headteacher / Principal / Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal Online Safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive regular monitoring reports from the Online Safety leader

The Online Safety Leader

- takes day to day responsibility for Online Safety issues and has a leading role in establishing and reviewing the school Online Safety policies / documents;

- ensures that all staff are aware of the procedures that need to be followed in the event of an Online Safety incident taking place;
- provides, or arranges, training and advice for staff;
- liaises with the Local Authority / relevant body;
- liaises with school technical staff;
- receives reports of Online Safety incidents and creates a log of incidents to inform future Online Safety developments;
- monitors Online Safety concerns on the VLE
- attends , where appropriate, committee or governors meetings;
- reports regularly to Senior Leadership Team

Network Manager / Technical Staff

The Network Manager / Technical Staff / Subject Leader for Computing is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required Online Safety technical requirements and any Local Authority / other relevant body Online Safety Policy / Guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy
- the filtering policy is applied and updated on a regular basis
- that they keep up to date with Online Safety technical information in order to effectively carry out their Online Safety role and to inform and update others as relevant
- that the use of the network / internet / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher ,Senior Leader or Online Safety leader for investigation / action / sanction
- that monitoring software / systems are implemented and updated as agreed in school policies

Teacher, Support and Other Staff

are responsible for ensuring that:

- they have an up to date awareness of Online Safety matters and of the current school Online Safety policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem to the Headteacher / Senior Leader / Online Safety leader for investigation / action / sanction
- all digital communications with pupils / parents / carers should be on a professional level and only carried out using official school systems
- Online Safety issues are embedded in all aspects of the curriculum and other activities
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Child Protection / Safeguarding Designated Person

The designated person should be trained in Online Safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

Pupils

- are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Policy
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good Online Safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school

Parents and Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, the website and providing information about national / local Online Safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good Online Safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website and online student pupil data if applicable

Third Party and Community Users

Community Users who access school systems / website as part of the wider school / academy provision will be expected to sign a Community User Acceptable Use Policy before being provided with access to school systems.

Appendices:

Appendix	Description
A	Pupil Acceptable Usage Agreement – Younger Pupils
B	Pupil Acceptable Usage Agreement – Older Pupils
C	Staff Acceptable Usage Agreement
D	Third Party / Volunteers Acceptable Usage Policy

Appendix A
The Partnership of St Edmunds and St Josephs
Pupil Acceptable Use Policy – for younger pupils (Foundation / KS1)

This is how we stay safe when we use computers:

I will ask a teacher or suitable adult if I want to use the computers

I will only use activities that a teacher or suitable adult has told or allowed me to use.

I will take care of the computer and other equipment

I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong.

I will tell a teacher or suitable adult if I see something that upsets me on the screen.

I know that if I break the rules I might not be allowed to use a computer.

Child's name…………..................

Signed (child):………………………………………………

Signed (parent): ……………………………………………..

Appendix B
The Federation of St Edmunds and St Josephs

Pupil Acceptable Use Policy – for older pupils

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other digital 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.

The school will ensure that pupils will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

For my own personal safety:

- I understand that the school will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, 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 be aware of “stranger danger”, when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc)
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the school systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- 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 use the school systems or devices for on-line gaming unless I have permission of a member of staff to do so.

I will act as I expect others to act toward me:

- I will respect others’ work and property and will not access, copy, remove or otherwise alter any other user’s files, without the owner’s knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions. This may be on any communication devices including wearable technology.
- I will not take or distribute images of anyone without their permission.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:

- I will only use my own personal devices (mobile phones / USB devices etc) in school if I have permission. I understand that, if I do use my own devices in the school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.

- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I 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 immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person / organisation who sent the email, 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 not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.

When using the internet for research or recreation, I recognise that:

- I should 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 try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the school network / internet, contact with parents and in the event of illegal activities involvement of the police.

Please complete the sections on the next page to show that you have read, understood and agree to the rules included in the Acceptable Use Policy. If you do not sign and return this agreement, access will not be granted to school systems and devices.

Pupil Acceptable Use Agreement Form

Please complete the sections below to show that you have read, understood and agree to the rules included in this Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school ICT systems.

I have read and understand the above and agree to follow these guidelines when:

- I use the school systems and devices (both in and out of school)
- I use my own devices in the school (when allowed) eg mobile phones, gaming devices USB devices, cameras etc
- I use my own equipment out of the school in a way that is related to me being a member of this school, eg communicating with other members of the school, accessing school email, website etc.

Name of Student / Pupil

Group / Class

Signed

Date

Parent / Carer Countersignature

Signed (parent): …………………………………………..

Appendix C
The Federation of St Edmunds and St Josephs

Staff (and Volunteer) Acceptable Use Policy Agreement

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. All users should have an entitlement to safe internet access at all times.

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 ICT 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 ICT in their everyday work.

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

Acceptable Use Policy Agreement

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

For my professional and personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of the Federation's ICT systems (eg laptops, email, etc) out of school, and to the transfer of personal data (digital or paper based) out of school.
- I understand that the school's ICT 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.
- 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. If I suspect my password is known I must change my password immediately, or request support in doing this.
- I will immediately report any illegal, inappropriate or harmful material or incident I become aware of, to the appropriate person.

I will be professional in my communications and actions when using the Federation's 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) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use chat and social networking sites in school in accordance with the school's policies.
- I will only communicate with pupils 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 or bring the school or those within school in to disrepute.

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

- When I use my mobile devices (laptops / 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 Federation about such use. I will ensure that any such devices are protected by encryption, up to date anti-virus software and are free from viruses.
- 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, by saving to the school network in accordance with relevant Federation 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 install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in the Federation policies.
- 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 (and other relevant policies). 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.

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).

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 Federation ICT equipment in school, but also applies to my use of Federation ICT 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 and other school policies relating to the use of technology I could be subject to disciplinary action. This could include 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 Federation ICT systems (both in and out of Federation schools) and my own devices (in Federation schools and when carrying out communications related to the Federation) within these guidelines.

Staff / Volunteer Name	
Signed	
Date	

Appendix D
The Federation of St Edmunds and St Josephs

Acceptable Use Policy for Third Party/Volunteer Users

This Acceptable Use Policy is intended to ensure:

- that community users of school digital technologies will be responsible users and stay safe while using these systems and devices
- that school systems, devices and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that users are protected from potential risk in their use of these systems and devices

Acceptable Use Policy

I understand that I must use school systems and devices in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems, devices and other users. This agreement will also apply to any personal devices that I bring into the school

- I understand that my use of school systems and devices and digital communications will be monitored
- I will not use a personal device that I have brought into school for any activity that would be inappropriate in a school setting.
- 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 immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- I will not access, copy, remove or otherwise alter any other user's files, without permission.
- I will ensure that if I take and / or publish images of others I will only do so with their permission. I will not use my personal equipment to record these images, without permission. If images are published it will not be possible to identify by name, or other personal information, those who are featured.
- I will not publish or share any information I have obtained whilst in the school on any personal website, social networking site or through any other means, unless I have permission from the school.
- I will not, without permission, 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 install or attempt to install programmes of any type on a school device, nor will I try to alter computer settings, unless I have permission to do so.
- I will not disable or cause any damage to school / academy equipment, or the equipment belonging to others.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- 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).
- I understand that if I fail to comply with this Acceptable Use Policy, the school has the right to remove my access to school systems / devices

I have read and understand the above and agree to use the school ICT 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.

Name

Signed Date