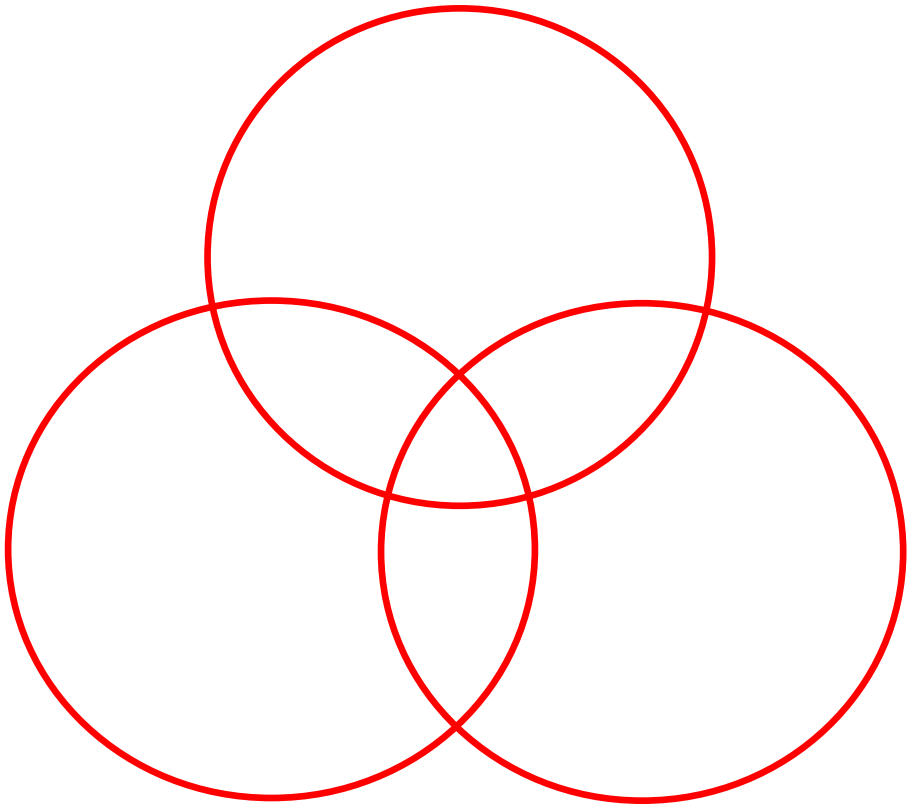
St Edmund's RC Primary School



Online Safety Policy

As a Catholic school we recognise in everyone the dignity and beauty of the person, made in the image of God. We value each individual and respect them regardless of their background and circumstances because they are our brothers and sisters in the family of God, and we are called to love and value everyone.

Introduction

This policy, with its two appendices (the Acceptable Usage Policy for Pupils and Acceptable Usage Policy for Staff) is used to educate and protect pupils and staff in their use of technology and to provide the appropriate mechanisms to intervene and to deal with any incidents that may arise. It should be read alongside the following policies:

- Computing
- Anti-Bullying
- Safeguarding
- Behaviour

Scope of the Policy

This policy applies to all members of the school community (including staff, pupils, volunteers, parents and carers, visitors) who have access to and are users of school ICT systems, both in and out of the school.
The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other online incidents covered by this policy, which may take place outside of the school, but are linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.
The school will deal with such incidents within this policy and associated Behaviour and Anti-Bullying policies and will, where known, inform parents and carers of incidents of inappropriate online behaviour that take place out of school.

Roles and Responsibilities

Governors are responsible for the approval of the Online Policy and for reviewing the effectiveness of the policy.

The Headteacher has a duty of care for ensuring the safety (including online) of members of the school community. The Headteacher is aware of the procedures to be followed in the event of a serious online allegation being made against a member of staff**.**

The Computing Subject Leader:

- takes day to day responsibility for online issues
- has a leading role in establishing and reviewing the school online safety policy and documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online incident taking place.
- provides training and advice for staff
- liaises with school technical support staff provided by 123ICT
- receives reports of online incidents and creates a log of incidents to inform future online developments

It is the responsibility of the school to ensure that the **technical service provider (123ICT)** ensures:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required online technical requirements and any Local Authority Online Policy/Guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- that the school keeps up to date with online technical information in order to effectively carry out their online role and to inform and update others as relevant
- that the use of the network, internet and email is regularly monitored in order that any misuse or attempted misuse can be reported to the Headteacher for investigation, action or sanction.

Teaching and Support Staff are responsible for ensuring that:

- they have an up-to-date awareness of online matters and of the current school online policy and practices
- they have read, understood and signed the Acceptable Usage Policy for staff
- they report any suspected misuse or problem to the Headteacher for investigation, action or sanction
- all digital communications with pupils, parents and carers should be on a professional level and only carried out using official school systems
- online issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the online and acceptable use policies
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- 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

The Child Protection / Safeguarding Designated Person should be trained in online 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

Parents and Carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. Parents and carers will be encouraged to support the school in promoting good online practice and to follow guidelines on the appropriate use of digital and video images taken at school events.

Pupils are responsible for using the school digital technology systems in accordance with the Acceptable Usage Policy for Pupils.

Education and training

Relevant and age-appropriate online messages are taught and revisited across the curriculum, in particular during Computing and PHSE lessons. Pupils are helped to understand the need for the Acceptable Usage Policy for Pupils and are encouraged to adopt safe and responsible use both within and outside of school.

Pupils are taught to be critically aware of the content they access online and be guided to validate the accuracy of information. They are also taught to acknowledge the source of information used for research, rather than copying information and presenting it as their own work. 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.

All staff receive online training in order that they understand their responsibilities as outlined in this policy.

Technical: infrastructure, equipment, filtering and monitoring

It is the responsibility of the school to ensure that the **technical service provider (123ICT)** carries out all the following online measures:

- School technical systems are managed in ways that ensure that the school meets recommended technical requirements
- Software licence logs are accurate and up to date
- Internet access is filtered for all users.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. The school infrastructure and individual workstations are protected by up to date virus software.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. 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 particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

In accordance with guidance from the Information Commissioner's Office, parents and carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). 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 and carers comment on any activities involving other 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.

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.

Personal Data

Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulations (2018):

- Fairly and lawfully processed

- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with high level protection such as encryption.

St Edmund's Catholic Primary School ensures that:

- all staff users have individual log-in details
- storage of all data within the school conforms to the UK data protection requirements and subsequent General Data Protection Regulation (GDPR)
- students and staff using mobile technology, where storage of data is online, will conform to the EU data protection directive where storage is hosted within the EU

The school must ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Storage of all data within the school will conform to the UK data protection requirements and subsequent General Data Protection Regulation (GDPR).
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the "Privacy Notice"
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data

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.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

Communications

The Oxfordshire County Council school email system may be regarded as safe and secure and is monitored.

Users must report to the Headteacher 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 must be professional in tone and content.

Social Media - Protecting Professional Identity

All schools and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured

party. Reasonable steps to prevent predictable harm must be in place. 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:

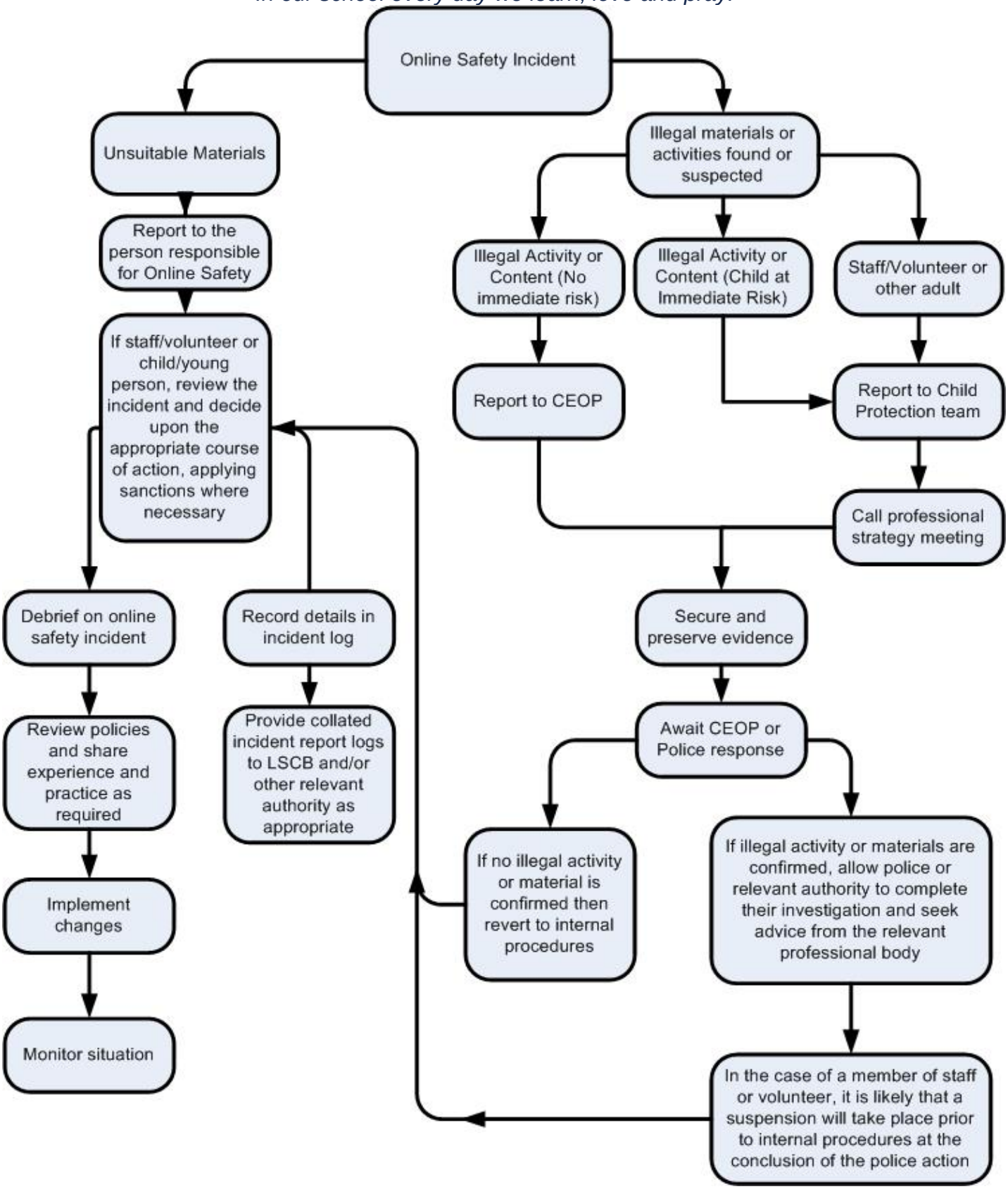
- No reference should be made in social media to pupils, parents and carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Unsuitable / inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are, however, a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

Responding to incidents of misuse

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart below for responding to online safety incidents and report immediately to the police.



It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, 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 young people 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.

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through the Behaviour Policy

[This policy is based on a template provided by The South West Grid for Learning Trust.]

Policy written: **January 2015**
Reviewed: **January 2019**
Reviewed: **May 2022**
Next review: **May 2025**

Appendix One: **Acceptable Usage Policy for Pupils**
Appendix Two: **Acceptable Usage Policy for Staff**

In our school every day we learn, love and pray.

Acceptable Usage Policy for Pupils

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 will always follow these guidelines, in and out of school, when I am accessing the internet on a computer and other devices.

If I see, hear or read anything which makes me feel uncomfortable I will tell a teacher or another adult.

I will be careful what I say to other people and how I say it:

- **I will not share my (or other people's) full name, address, telephone number or any personal information online.**
- **I will remember that online people can pretend to be someone else and may not be as friendly as they seem. I will not arrange to meet up with someone I have only spoken to online.**
- **I will make sure I am respectful and polite. I will not use bad or unkind language and I will not send or store upsetting pictures and images.**

I will keep passwords secret and only use my own logins.

I will only access websites which are appropriate for use in school.

When using school equipment, I will check with a teacher before sending emails, opening attachments, downloading files or filling in forms.

When I find information on the internet:

- **I will remember that some information on the internet is not accurate.**
- **I will not copy information or pictures from the internet and pretend that it is my own work.**

I will close down the internet browser and log off the computer when my session has finished.

My parents and I have read the Online Acceptable Usage Policy and I agree to follow it.

Pupil's Name: _____

Pupil's Signature: _____

In our school every day we learn, love and pray.

Parent / Carer Acceptable Use Agreement

This Acceptable Use Policy is intended to ensure:

• that young people 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 parents and carers are aware of the importance of online and are involved in the education and guidance of young people with regard to their online behaviour.

The school will try to 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. A copy of the Acceptable Usage Policy for Pupils is attached to this permission form, so that parents and carers will be aware of the school expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

Permission Form

Parent / Carers Name: _____ Pupil Name: _____

As the parent / carer of the above pupil, I give permission for my son / daughter to have access to the internet and to ICT systems at school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I will ensure that any USB devices my child uses to bring homework into school are protected by up to date anti-virus software and are free from viruses.

I understand that my son's / daughter's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I understand that if he/she fails to follow the Online Acceptable Usage Policy that his/her internet access may be withdrawn, and I will be informed.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online.

Signed: _____ Date: _____

Acceptable Usage Policy for Staff

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 online 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 school ICT systems (e.g. laptops, email) out of school, and to the transfer of personal data (digital or paper based) out of school
• I understand that the school 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.
• 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 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. Where these images are published (e.g. on the school website) it will not be possible to identify by name, or other personal information, those who are featured.
• 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 online activity that may compromise my professional responsibilities.

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 / 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 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 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 school 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 (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 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:
• 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 school ICT equipment in school, but also applies to my use of school 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, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors 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 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.

Staff Name: _____

Signed: _____

Date: _____