Christ the Sower Ecumenical School
E-Safety Policy

Vision statement

At Christ the Sower Ecumenical Primary School we provide the 'good earth' for all our children to flourish; where every child can learn and explore who they are created to be, with the high expectation that we, individually and collectively, will enable every child to be and do the best they can.
A loving place where we all care, learn and grow together.

Members of staff responsible:

All staff

Date of policy: Spring 2021

Policy Intent

Christ the Sower is committed to the use of computer technologies and recognise access to the internet as a valuable tool for learners of all ages. The internet is increasingly providing the focal point of educational content within the UK. However, the school recognises that computers and the internet do have the potential for inappropriate use and access to undesirable material and that we have a duty of care to protect our pupils.

We are clear that all pupils should use computers including the internet, as an essential part of the planned curriculum and as a natural part of the modern learning opportunities within our school. However, we will educate our pupils about E-safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies in and beyond the context of the classroom.

Our Online Safety Policy is based on the following key principles:

- ensure pupils' internet use and access is appropriate and controlled.
- preventing misuse of internet connected devices.
- ensuring pupils and parents/carers are educated on the risks carried with internet use and how to minimise and deal with those risks.
- providing students with knowledge and resources to make decisions to ensure their safety online

- ensuring procedures and access is effectively managed to minimise risks

The term E-Safety refers to all aspects of the taught and untaught curriculum and in the home, where children and young people communicate using electronic media, fixed and mobile devises which have access to the internet. It focuses on ensuring that children and young people are protected from harm and supported to achieve the maximum benefit from new and developing technologies without risk to themselves or others.

Policy Implementation

All users of the school computing network must sign an Acceptable Use Agreement.

1. Pupils

1.1. The education of pupils in E-safety is an essential part of the school's curriculum provision. Christ the Sower believes children and young people need help and support plus a well-planned curriculum to recognise and avoid E-safety risks and build their resilience. E-safety should be a focus in all areas of the curriculum and the E-safety message reinforced across the curriculum.

- A planned E-safety curriculum as part of Computing/IT, PHSE and other lessons and is regularly revisited and reinforces in assemblies and other activities
- Pupils are taught in all lessons to be critically aware of the materials and content they access on-line and be guided to validate the accuracy of information.
- Pupils are supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- Pupils are taught to respect copyright when using material accessed on the internet
- Pupils are helped to understand the need for the Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff act as good role models in their use of digital technologies, the internet and mobile devices
- Pupils are 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.
- Staff are vigilant in monitoring the content of the websites the young people visit.
- Where pupils research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

2. Parents / Carers

2.1. CtS will offer and provide information and awareness to parents and carers through a range of communications, and sources of advice and support. This may include:

- Curriculum activities

- Letters, newsletters, web site,
- Virtual Learning Platforms
- Parents / Carers information sessions
- High profile events and campaigns e.g. Safer Internet Day
- Reference to the relevant E-safety web sites / publications as appropriate

3. The Wider Community

The school website will provide E-safety information and advice for the wider community.

4. Staff, Governors and Volunteers

4.1. CtS will offer training, induction and updates and for E-safety to feature in the schools monitoring work. This will include:

- E-safety to be a feature of induction programmes for new volunteers and staff ensuring that they fully understand the school E-safety policy and Acceptable Use Agreements.
- A planned programme of formal E-safety training to be made available to staff with regular updates and reinforcement.
- An audit of the E-safety training needs of all staff will be carried out annually.
- On line safety may feature in some staff performance reviews
- Ensure E-safety Coordinator receives regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations through headteacher reports and reports from the E-safety Coordinator.
- The E-safety policy and its updates are presented to and discussed by staff in staff meetings and INSET days.
- The E-safety Coordinator provides advice, guidance and training to individuals as required.
- Attendance at training provided by external organisations
- Participation in school training sessions for staff or parents (this may include attendance at assemblies / lessons).

5. Use of digital and video images

5.1. Christ the Sower is aware that 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. Such images may

- provide avenues for cyberbullying to take place
- remain available on the internet forever
- cause harm or embarrassment to individuals in the short or longer term.

5.2. Cts will inform and educate users about these.

5.3. Written permission from parents or carers will be obtained before photographs of pupils are published on the school website/social media/local press

5.4. When using digital images, staff will 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.

5.5. Images of children in school should only be taken on school equipment. The personal equipment of staff should not be used for such purposes.

5.6. We do not allow parents/carers to take photos or recordings of children during Collective Worship or school trips and events in or out of the classroom. Recordings and photos may be made of specific productions, when approved by the Headteacher, Parents/carers will be reminded that no recordings or photos of school productions can be shared on any social media platform without the direct permission of the parent/carer of the child involved.

5.7. The following apply when taking photos or recordings:

- 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/academy 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 students/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.

5.8 Video calling during remote learning-
The school may use either Microsoft teams or Google Meet in Google Classroom for small groups of children/classes. Virtual meetings may also be held with parents

- The parent or carer must make sure their child and other members of the household are aware the video call is happening. The parent should stay in the room. Two members of school staff will be on each call.
- Children or parents should not take screen shots of the call.
- For GDPR reasons, children should use only first names on a call. When meeting with parents remotely, we will ask them to use surnames only e.g. Mr Jones.
- Staff, children and other members of the household must wear suitable clothing
- Devices used should be in appropriate areas, for example, not in bedrooms; and where possible be against a neutral background. Children may be asked to switch off video cameras for safeguarding purposes

- Language must be professional and appropriate, including any family members in the background.
- The same expectations apply for remote teaching and conversations as normal school conduct
- Staff will only ever video call a pupil with prior agreement with parents and the head teacher or deputy. This will always be at a pre-arranged time.
- The waiting room function will be used and private messaging dis functioned

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

- The official school email service is regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.
- 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, social media, chat, blogs, VLE etc) must be professional in tone and content.

6. Unsuitable / inappropriate activities

6.1. Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

- Child sexual abuse images –The making, production or distribution of indecent images of children.
- Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.
- Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008
- Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986
- Pornography
- Promotion of any kind of discrimination
- Threatening behaviour, including promotion of physical violence or mental harm
- Promotion of extremism or terrorism
- Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute

Such action could lead to criminal prosecution.

6.2. Activities that might be classed as cyber-crime under the Computer Misuse Act:

- Gaining unauthorised access to school networks, data and files, through the use of computers/devices
- Creating or propagating computer viruses or other harmful files

- Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)
- Disable/Impair/Disrupt network functionality through the use of computers/devices
- Using penetration testing equipment (without relevant permission)

6.3. In addition there are 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.

6.4. Users should not engage in these activities when using school equipment:

- Using school systems to run a private business
- Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy
- Infringing copyright
- Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)
- Creating or propagating computer viruses or other harmful files
- Unfair usage (downloading / uploading large files that hinders others in their use of the internet)
- On-line gaming (non-educational)
- On-line gambling
- On-line shopping/commerce
- File sharing
- Use of messaging apps]
- Use of video broadcasting e.g. Youtube

Responding to incidents of misuse

Illegal Incidents

6.5. 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 in Appendix H for responding to online safety incidents and report immediately to the police.

Other Incidents

6.6. All members of the school community are expected to 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.

6.7. **In the event of suspicion, senior leaders and governors should act promptly and to take all the steps in this procedure:**

- Have more than one senior member of staff and/or governor involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the investigation 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.
- Ensure during the investigation that the sites and content visited are closely monitored and recorded (to provide further protection); recording the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may 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 record (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the individual 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 ODBST officers or national/local organisations (as relevant).
    - Police involvement and/or action

- **If the 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
    - promotion of terrorism or extremism
    - offences under the Computer Misuse Act (see Appendix H)
    - 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.**

6.8. It is important that all 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 any associated paperwork should be retained by the investigating panel for evidence and reference purposes.

7. School Actions & Sanctions

7.1. It is more likely that our 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 pupils are aware of the standards in place to minimise any breaches. It is expected that incidents of misuse will be dealt with through normal behaviour policies and procedures.

7.2. The school is aware that staff conduct policies need to recognise and reflect similar infringements by adults, employees and volunteers and will keep such ODBST/CtS policies under review.

8. Other Associated Polices

8.1. . These include but are not restricted to:

- ODBST CtS Safeguarding and Child Protection Policy
- COVID19 School Safeguarding Policy Annex
- ODBST Remote Learning Safeguarding Checklist
- ODBST CtS Remote Learning Policy
- ODBST Remote Learning Guidance
- ODBST CtS Code of Conduct for Staff
- Mobile Phone Policy
- ODBST CtS Social Media Policy
- ODBST CtS Data Protection Policy
- ODBST E-safety Policy Guidance

Appendices

The following appendices will be adopted into the school's E-safety policy.

Each can be copied onto school headed paper and adjusted to suit the age and stage of pupils or the intended audience.

A. Pupil Acceptable Use Agreement Template – for younger pupils (Foundation/KS1)
B. Pupil Acceptable Use Policy Agreement Template – for older pupils (KS2)
C. Parent/Carer Acceptable Use Agreement Template
D. Staff (and Volunteer) Acceptable Use Policy Agreement Template
E. Acceptable Use Agreement for Community Users Template
F. Summary of Types of Communication
G. Summary of Unsuitable/ Inappropriate Activities
H. Responding to incidents of misuse – flow chart
I. Technical – infrastructure, equipment, filtering and monitoring

Appendix A

Pupil Acceptable Use Policy Agreement – 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 / tablets
- 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 / tablet

Signed (child):…….

Appendix B

Pupil Acceptable Use Agreement Form for older pupils (KS2)

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

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
- 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 intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- I will not 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, on-line gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube).

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

- 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.
- 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 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 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.
- I will only use social media sites with permission and at the times that are allowed

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 may lose access to the school network, receive other sanctions and my teacher may contact my parents. In the event of illegal activities this may involve the police.

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)

Name of Pupil: .....

Group / Class: .....

Signed: .....

Date: .....

Appendix C

Parent / Carer Acceptable Use Agreement – Template

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

Either: (KS2 and above)

I know that my son / daughter has signed an Acceptable Use Agreement and has received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

Or: (KS1)

I understand that the school has discussed the Acceptable Use Agreement with my son / daughter and that they have received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of 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 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 understand that my son's / daughter's activity on the 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 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 safety.

As the parent / carer of the named pupil, I agree to the school taking and using digital / video images of my child / children. I understand that the images will only be used to support learning activities or in publicity that reasonably celebrates success and promotes the work of the school.	Yes / No
I agree that if I take digital or video images at, or of – school events which include images of children, other than my own, I will abide by these guidelines in my use of these images.	Yes / No

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

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.

Parent / Carers Name: .....

Date: ……

Pupil Name:.....

Appendix D

Staff (and Volunteer) Acceptable Use Policy Agreement Template

This Acceptable Use Policy is intended to ensure:

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

The school will try to ensure that staff and volunteers will have good access to digital technology 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 systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that students / pupils receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the school / academy will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, VLE etc.) out of school, and to the transfer of personal data (digital or paper based) out of school (schools / academies should amend this section in the light of their policies which relate to the use of school systems and equipment out of school)
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school. (schools should amend this section in the light of their policies which relate to the personal use, by staff and volunteers, of school systems)
- 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 / academy 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 (e.g. on the school website

/VLE) it will not be possible to identify by name, or other personal information, those who are featured.

- I will only use social networking sites in school in accordance with the school's policies. (schools / academies should amend this section to take account of their policy on access to social networking and similar sites)
- I will only communicate with students / pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner. (schools should amend this section to take account of their policy on communications with students / pupils and parents / carers. Staff should be made aware of the risks attached to using their personal email addresses / mobile phones / social networking sites for such communications)
- I will not engage in any on-line activity that may compromise my professional responsibilities.

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

- When I use my mobile devices (laptops / tablets / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules which may be set by the school's Local Governing Body about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the school ICT systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email.
- I will ensure that my data is regularly backed up, in accordance with 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 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 General Data Protection Regulations require 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 loss of such data and 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 school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action as set down in Trust HR policies and in the event of illegal activities the involvement of the police.

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

Staff / Volunteer Name:

……..

Signed: …….

Date: ……

Appendix E

Acceptable Use Agreement for Community Users Template

This Acceptable Use Agreement 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 Agreement

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 / academy:

- 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 Agreement, the school / academy has the right to remove my access to school systems / devices

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

Name: .....

Organisation: ……

Signed: .....

Date: .....

Appendix F

Summary of Types of Communication
The following table shows what may and may not be used at school:

	STAFF				OTHER ADULTS			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff	Not allowed
Mobile phones may be brought to school but kept out of sight of pupils and parents and kept on silent	X				X			
Use of mobile phones in lessons or in playground				X				X
Use of mobile phones in social time	X				X			
Mobile phones should be taken on educational visits by staff so they can contact the office and the other leader in an emergency	X							
Taking photos of children on personal devices				X		X		
Use of school electronic devices	X					X		
Use of personal email addresses in school, or on school network		X						X
Use of school email for personal emails		X						X
Use of chat rooms				X				X
Use of instant messaging				X				X
Use of social networking sites				X				X
Use of blogs outside of the School's blogs				X				X

Pupils are not permitted to bring mobile phones into school. Should it be necessary for before and after school contact, this should be discussed with the Office Manager and the phone kept in the office.

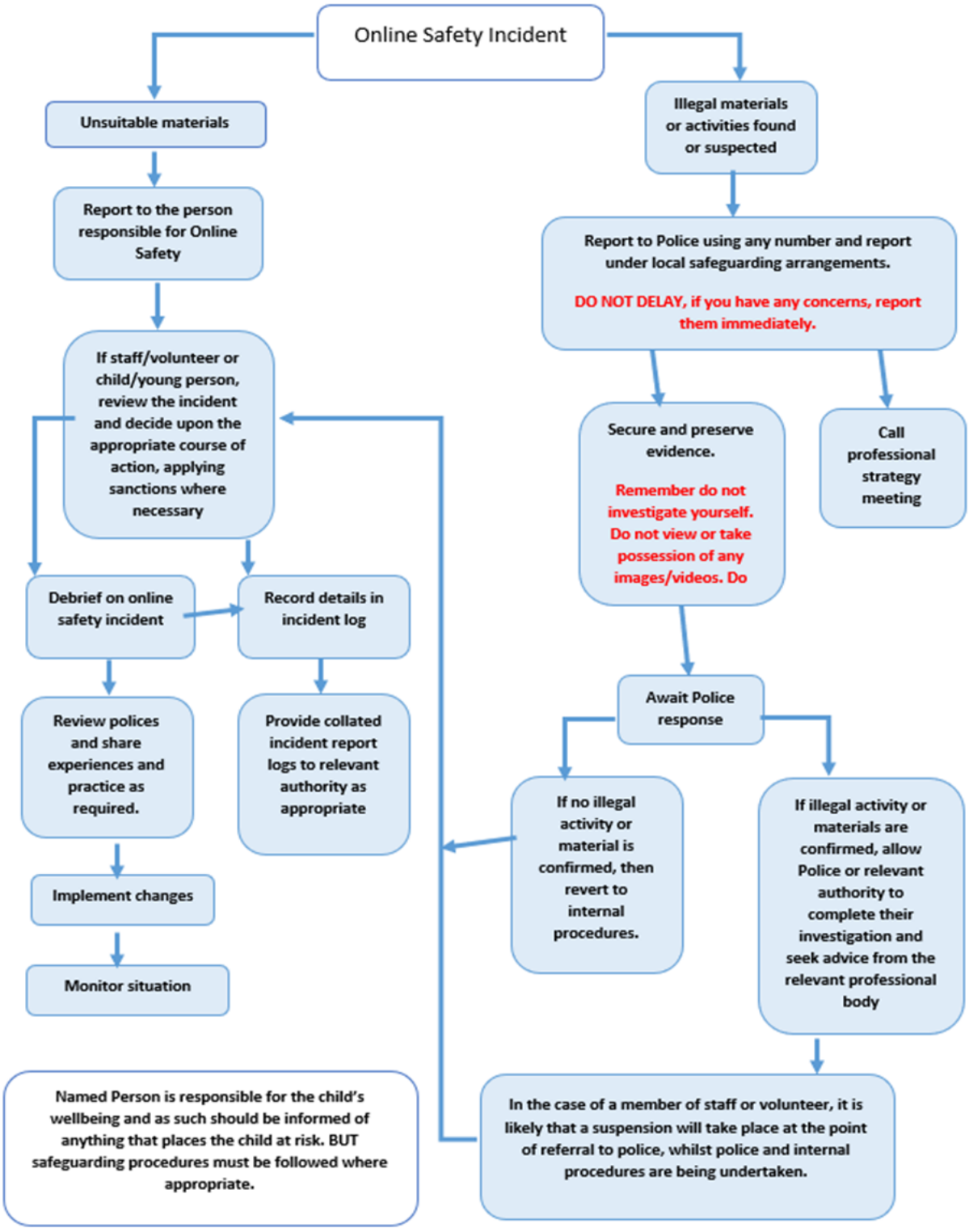
Appendix G

Summary of Unsuitable / Inappropriate Activities
The school policy restricts internet usage as follows:

User actions		Allowed at certain times	Allowed with staff permissi	Not allowed
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Sexually explicit images			X
	promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation			X
	adult material that potentially breaches the Obscene Publications Act in the UK			X
	Any material deemed to be racist, discriminatory, pornographic or religious hatred			X
	threatening behaviour, including promotion of physical violence or mental/emotional abuse or harm			X
	any other information which may be offensive to colleagues, breaches the integrity of the ethos of the school or brings the school into disrepute			X
Using school systems to run a private business				X
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by BucksGfL and / or the school				X
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions				X
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)				X
Creating or propagating computer viruses or other harmful files				X
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet			X	
On-line gaming (educational)		X		
On-line gaming (non educational)			X	
On-line gambling				X
On-line shopping / commerce			X	
File sharing			X	
Use of social networking sites				X
Use of video broadcasting eg Youtube			X	

Appendix H

Responding to incidents of misuse – flow chart



Appendix I

Technical – infrastructure equipment, filtering and monitoring

- Christ the Sower has a managed ICT service provided by an outside contractor which is supported by an ICT technician. It is the responsibility of the Local Governing Body to ensure that the managed service provider carries out all the E-safety measures that would otherwise be the responsibility of the school. It is also important that the managed service provider is fully aware of the trust's and school's E-safety Policy and the agreed Acceptable Use Agreements.
- It is the devolved responsibility of the LGB to ensure that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved are implemented. It will also need to ensure that the relevant people are effective in carrying out their E-safety responsibilities:
- The ODBST & Christ the Sower will ensure that:
- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of school academy technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.
- All users (at KS2 and above) will be provided with a username and secure password. Users are responsible for the security of their username and password (Group or class log-ons and passwords for KS1 and below may be used, but there needs to be an awareness of the associated risks)
- The "master / administrator" passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the Headteacher or other nominated senior leader and kept in a secure place (e.g. school safe)
- A named individual is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- Internet access is filtered for all users and content lists are regularly updated and internet use is logged and regularly monitored.
- Internet filtering/monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet.
- There is a clear process in place to deal with requests for filtering changes
- The school has provided enhanced/differentiated user-level filtering (allowing different filtering levels for different ages and different groups of users – staff, pupils, parents etc.)
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.
- Teaching about the responsibilities of internet use should include an awareness that:
- School technical staff regularly monitor and record the activity of users on the school technical systems

- A system is in place for users to report any technical incident or security breach to the relevant person.
- Security measures are in place to protect the school's system from accidental or malicious attempts to access the school's systems and data.
- The extent of personal use that users and their family members are allowed on school devices
- The use of removable media (e.g. memory sticks) by users on school devices
- The encryption or otherwise of secured and personal data. School technical staff regularly monitor and record the activity of users on the school technical systems