ST. HILD'S
CHURCH OF ENGLAND SCHOOL

Policy Document

E-SAFETY

At St. Hild's we aim to serve our community by providing high quality education in a Christian context. We are a comprehensive school guaranteeing equal opportunities, a responsive curriculum and a supportive community. We expect to find God at work in our school.

The School is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment.

"I have come that they may have life in all its fullness (John 10:10)"

Contents: **Page**

Introduction & Aims 1
Roles and Responsibilities 2-4
Education and Training 4
AUA 4
Copyright 5
Staff Training 5
Communication 5
Social Networking Sites 6
Digital Images 6
Removable Data Storage Devices 6
Websites 6-7
Passwords 7
Use of Own Equipment 7
Use of School Equipment 7
Monitoring 8

Introduction and Aims

The purpose of this policy is to establish the ground rules we have in St Hild's Church of England School for using ICT equipment and the Internet.

New technologies have become integral to the lives of children and young people in today's society, both within educational establishments and in their lives outside school. The Internet and other digital/information technologies are powerful tools which open up new opportunities for everyone.

Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe Internet access at all times. The requirement to ensure that children and young people are able to use the Internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. This e-safety policy will help to ensure safe and appropriate use. The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement. However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content.
- Unauthorised access to, loss of or sharing of personal information.
- The risk of being subject to grooming by those with whom they make contact on the Internet.
- The sharing/distribution of personal images without an individual's consent or knowledge.
- Inappropriate communication/contact with others, including strangers.
- Cyber-bullying.
- Access to unsuitable video/Internet games.
- An inability to evaluate the quality, accuracy and relevance of information on the Internet.
- Plagiarism and copyright infringement.
- Illegal downloading of music or video files.
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is read and used in conjunction with other school policies; specifically Anti-Bullying, Behaviour and Safeguarding.

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision, to build pupils' resilience to the risks to which they may be exposed so that they have the confidence and skills to face and deal with these risks.

The school provides the necessary safeguards to help ensure that we have done everything that could reasonably be expected to manage and reduce these risks. The e-safety policy explains how the school intends to do this, whilst also addressing wider educational issues in order to help young people (and their parents/carers/staff) to be responsible users and stay safe while using the Internet and other communications technologies for educational, personal and recreational use.

Scope

This policy applies to all members of the school community (including staff, pupils, governors, volunteers, parents/carers and visitors) who have access to and are users of school ICT systems, both in and out of 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 e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school. The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate e-safety behaviour that take place out of St Hild's Church of England School.

Roles & Responsibilities

This section outlines the roles and responsibilities for e-safety of individuals and groups within the School.

Governors (IEB)

Governors are responsible for the approval of the e-safety policy and for reviewing the effectiveness of the policy. A member of the Governing Body has taken on the role of E-Safety Governor. The role of the E-Safety Governor will include:

- Meetings with the ICT Technicians and E-Safety Coordinator(s)
- Regular monitoring of e-safety incident logs
- Monitoring of filtering/change control logs
- Reporting to relevant Governors (IEB) and/or committee(s) meetings.

Headteacher & Senior Leadership Team (SLT)

The Headteacher is responsible for ensuring:

- The safety (including e-safety) of all members of the school community, although the day to day responsibility for e-safety may be delegated to the E-Safety Coordinator
- Adequate training is provided
- Effective monitoring systems are set up
- That relevant procedure in the event of an e-safety allegation are known and understood.
- Establishing and reviewing the school e-safety policies and documents (in conjunction with e-safety co-ordinator)
- The school's Designated Child Protection Officer(s) should be trained in e-safety issues and be aware of the potential for serious child protection issues to arise through the use of ICT.

E-Safety Co-ordinator (ESC)

A member of the School has taken on the role of E-Safety Coordinator. The E-Safety Co-ordinator takes day to day responsibility for e-safety issues and has a leading role in:

- Liaising with staff, the LA, Safeguarding Team, ICT Technical staff, E-Safety Governor and SLT on all issues related to e-safety;
- Ensuring that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place;

- Providing training and advice for staff;
- Receiving reports of e-safety incidents and creates a log of incidents to inform future e-safety developments;
- Co-ordinating and reviewing e-safety education programme in school
- Delivering of up to date e-safety information to St Hild's pupils

ICT Technician(s)

The ICT Technicians- through the Managed Service (Dataspire) are responsible for ensuring that:

- The school's ICT infrastructure is secure and meets e-safety technical requirements
- The school's password policy is adhered to
- The school's filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- Co-ordinator keeps up to date with e-safety technical information
- The use of the school's ICT infrastructure (network, remote access, e-mail, VLE etc.) is regularly monitored in order that any misuse or attempted misuse can be reported to the E-Safety Coordinator and/or SLT for investigation/action/sanction.

.

Teaching & Support Staff

In addition to elements covered in the Staff Acceptable Usage Agreement (AUA), all teaching and support staff are responsible for ensuring that:

- They have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- They have read, understood and signed the school Staff Acceptable Usage Agreement (AUA)
- E-safety issues are embedded in all aspects of the curriculum and other school activities
- Pupils understand and follow the school's e-safety and acceptable usage policies
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They monitor ICT activity in lessons, extracurricular and extended school activities
- 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.
- Make use of school systems to monitor pupils' computer internet use whilst in lesson or after school clubs.

Pupils

- Are responsible for using the school ICT systems in accordance with the Pupil Acceptable Usage Agreement, which they will be required to sign before being given access to school systems. Parents/carers will be required to read through and sign alongside their child's signature.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's e-safety policy also covers their actions out of school, if related to their membership of the school.

Parents/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. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take opportunities to help parents/carers understand these issues. Parents and carers will be responsible for:

- Endorsing (by signature) the Pupil Acceptable Usage Agreement (AUA).
- Accessing the school website in accordance with the relevant school Acceptable Usage Agreement.
- Modelling good use of the internet.

Community Users

Community users who access school ICT systems/website as part of the
Extended School provision will be expected to sign and adhere to, an Adult/Volunteer User AUA (see Appendix 7) before being provided with access to school systems.

Governing Body Users

Governors (IEB) who access school ICT systems/website as part of the Governing Body will be expected to sign and adhere to, the Governor AUA (see Appendix 8) before being provided with access to school systems.

Education and Training

E-safety education will be provided in the following ways:

- A planned e-safety programme is provided as part of the form tutor and assembly programme and is regularly revisited in Information Communication Technology and other lessons across the curriculum – this programme covers both the use of ICT and new technologies in school and outside of school.
- Pupils are taught in lessons to be critically aware of the materials/content they access on-line and are guided to validate the accuracy of the information.
- Pupils are helped to understand the need for the Pupil AUA and encouraged to adopt safe and responsible use of ICT, the Internet and mobile devices both within and outside of school.
- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the Internet.
- Rules for the use of ICT systems and the Internet are posted in school
- Staff act as good role models in their use of ICT, the Internet and mobile devices.

Acceptable Usage Agreement (see Appendix 5/6/7)

- **Parents/carers** will be required to read through and sign alongside their child's signature, helping to ensure their children understand the rules
- **Staff and regular visitors/ volunteers** to the school have an AUA that they must read through and sign to indicate understanding of the rules.

Copyright

- Pupils are taught an appropriate understanding of research skills and the need to avoid plagiarism and uphold copyright regulations- staff to monitor this.
- Pupils are taught, appropriate to their age, to acknowledge the source of information used and to respect copyright when using material accessed on the Internet.
- If using a search engine for images – staff / pupils should open the selected image and go to it's website to check for copyright.

Staff Training

- E-Safety Coordinator(s) ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place
- A planned programme of e-safety training is available to all **staff**. An audit of the e-safety training needs of all staff will be carried out regularly.
- All new **staff** receive e-safety training as part of their induction programme, ensuring that they fully understand the school E-Safety policy, Acceptable Usage and Safeguarding Agreements
- The **E-Safety Coordinator/SLT link** will receive regular updates through Local Authority and/or other information/training sessions and by reviewing guidance documents released.
- **Governors** (IEB) are invited to take part in e-safety training and awareness sessions, with particular importance for those who are members of any committee or working group involved in ICT, e-safety, health and safety or child protection

Communication

Email

- Digital communications with pupils (e-mail, online chat, VLE, voice etc.) should be on a professional level and only carried out using official school email/ Twitter.
- The school's e-mail service should be accessed via the provided web-based interface by default (this is how it is set up for the laptops, school curriculum systems);
- Under no circumstances should staff contact pupils, parents/carers or conduct any school business using personal e-mail addresses.
- School e-mail is not to be used for personal use. Staff can use their own email in school (before, after school and during lunchtimes when not working with children) – but not for contact with parents/ carers or pupils.

Mobile Phones

- **School** mobile phones only should be used to contact parents/carers/pupils when on school business with pupils off site. Staff should not use personal mobile devices.
- **Staff** should not be using personal mobile phones in school during working hours when in contact with children.
- Students should adhere to the rules and guidelines set out in the Mobile Phone Expectations regarding mobile phone use in St Hild's Church of England School.

Social Networking Sites

Young people will not be allowed on social networking sites at school; at home it is the parental responsibility, but parents/carers should be aware that it is illegal for children under the age of 13 to be on certain social networking sites.

- **Staff** should not access social networking sites on school equipment in school or at home. Staff should access sites using personal equipment.
- **Staff** users should not reveal names of staff, pupils, parents/carers or any other member of the school community on any social networking site or blog**.**
- **Pupils/parents/carers** should be aware the School will investigate misuse of social networking if it impacts on the well-being of other pupils or stakeholders.
- If inappropriate comments are placed on social networking sites about the School or School staff then advice would be sought from the relevant agencies, including the police if necessary.
- Pupils in the KS3 curriculum will be taught about e-safety on social networking sites as we accept some may use it outside of school.

Digital Images

- The school record of parental permissions granted/not granted must be adhered to when taking images of our pupils. A list is published to all staff on a termly basis, but can also be obtained from the data office or the child protection officers in school.
- Under no circumstances should images be taken using privately owned equipment without the express permission of the Headteacher or SLT.
- Where permission is granted the images should be transferred to school storage systems (server or disc) and deleted from privately owned equipment at the earliest opportunity.
- Permission to use images of all staff who work at the school is sought on induction and a copy is located in the personnel file.

Although many of the above points are preventative and safeguarding measures, it should be noted that the school will endeavour whenever possible to use social networking in positive ways to publicise, inform and communicate information. The school has an active website and Twitter account which are used to inform, publicise school events and celebrate and share the achievement of pupils.

Removable Data Storage Devices

- All files downloaded from the Internet, received via e-mail or provided on removable media (e.g. CD, DVD, USB flash drive, memory cards etc.) must be checked for viruses using school provided anti-virus software before run, opened or copied/moved on to local/network hard disks.
- Pupils should not use their own removable data storage devices in school unless asked to do so by a member of staff.

Websites

- 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.
- Staff will preview any recommended sites before use.

- "Open" searches (e.g. "find images/ information on...") are discouraged when working with younger students who may misinterpret information.
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by staff. **Parents/carers** will be advised to supervise any further research.
- **All** users must observe copyright of materials published on the Internet.
- Teachers will carry out a risk assessment regarding which pupils are allowed access to the internet with minimal supervision. Minimal supervision means regular checking of the pupils on the internet by the member of staff setting the task. All staff are aware that if they pass pupils working on the internet that they have a role in checking what is being viewed. Pupils are also aware that all internet use at school is tracked and logged.
- The School only allows the E-Safety Co-ordinator, ICT technician(s) and SLT to access to Internet logs.

Passwords

Staff

- Passwords or encryption keys should not be recorded on paper or in an unprotected file
- Passwords should be changed at least every 3 months
- Users should not use the same password on multiple systems or attempt to "synchronise" passwords across systems

Pupils

- Should not let other pupils know their school password.
- Inform staff immediately if passwords are traced or forgotten. All staff are able to access the network to allow pupils to change passwords

Use of Own Equipment

- Privately owned ICT equipment should never be connected to the school's network without the specific permission of the Headteacher or ICT co-ordinator(s).
- Pupils should not bring in their own equipment unless asked to do so by a member of staff.

Use of School Equipment

- No personally owned applications or software packages should be installed on to St Hild's Church of England School ICT equipment;
- Personal or sensitive data (belonging to staff) should not be stored on the local drives of desktop, Ipads or laptop PCs. If it is necessary to do so, the local drive must be encrypted.
- All staff/pupils should ensure any screens are locked (by pressing Ctrl, Alt, Del simultaneously) before moving away from a computer during the normal working day to protect any personal, sensitive, confidential or classified data and to prevent unauthorised access.

Monitoring

All use of the school's Internet access is logged and the logs are randomly but regularly monitored by the School's Managed Service. Whenever any inappropriate use is detected it will be followed up by the E-Safety Co-ordinator, Year Leader, Progress Leader or members of the Senior Leadership Team depending on the severity of the incident.

- E-Safety Coordinator and ICT Technicians (Dataspire) record any breaches, suspected or actual, of the filtering systems

- Any member of staff employed by the School who comes across an e-safety issue must not investigate any further but immediately reports it to the e-safety co-ordinator(s) and impounds the equipment. This is part of the school safeguarding protocol. (If the concern involves the E-Safety Co-ordinator then the member of staff should report the issue to the Headteacher).

Incident Reporting

Any e-safety incidents must immediately be reported via CPOMS. The E-Safety Coordinator will investigate further following e-safety and safeguarding policies and guidance.

Responding to incidents of misuse

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place through careless or irresponsible, or very rarely, through deliberate misuse. Listed in Appendix 2 are the responses that will be made to any apparent or actual incidents of misuse. If any apparent or actual, misuse appears to involve illegal activity e.g. child sexual abuse images, adult material which potentially breaches the Obscene Publications Act, criminally racist material or other criminal conduct, activity or materials the Appendix table should be consulted. Actions will be followed in accordance with policy, in particular the sections on reporting the incident to the police and the preservation of evidence. If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. It is recommended that more than one member of staff is involved in the investigation which should be carried out on a "clean" designated computer. 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 normal behaviour/disciplinary procedures as follows (Appendix 3 for pupils and Appendix 4 for staff respectively). The school with will follow the Online Safety and misuse flow chart (Appendix 9)

Key people named in this Policy

- E-Safety Co-ordinator - Mr D Richardson
- E-Safety Governor - Mrs J Young

This policy should be read in conjunction with:

- Safeguarding Children & Child Protection Policy
- Anti-Bullying Policy
- Discipline & Student Behaviour Policy

Appendix 1

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks/disadvantages:

	Staff and other adults				Students and young people			
Communication Technologies	Permitted	Permitted at certain times	Permitted for named staff	Not Permitted	Permitted	Permitted at certain times	Allowed with staff permission	Not Permitted
Mobile phones may be brought to school	✓				✓			
Mobile phones used in lessons				✓		✓		
Use of mobile phones in social time	✓							✓
Taking photographs on mobile devices				✓				✓
Use of PDAs and other educational mobile devices	✓				✓			
Use of school email for personal emails				✓				✓
Use of social network sites			✓				✓	
Use of educational blogs	✓				✓			

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

- The official school email service may be regarded as safe and secure and is 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 need to be aware that email communications may be monitored
- Users must immediately report, to the nominated person (in accordance with the school policy) the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- 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 public chat/social networking programmes must not be used for these communications.
- Pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Appendix 2

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 ICT 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. The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts certain internet usage as follows. 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:

User actions	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Child sexual abuse images					✓
Promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation					✓
Adult material that potentially breaches the Obscene Publications Act in the UK					✓
Criminally racist material in the UK					✓
Pornography					✓
Promotion of any kind of discrimination				✓	
Promotion of racial or religious hatred					✓
Threatening behaviour, including promotion of physical violence or mental harm					✓
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				✓	
Using school systems to run a private business				✓	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by BMBC and / or the school				✓	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions				✓	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)				✓	
Creating or propagating computer viruses or other harmful files				✓	
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				✓	
On-line gaming (educational)		✓			
On-line gaming (non- educational)				✓	
On-line gambling				✓	
On-line shopping / commerce			✓		
File sharing			✓		
Use of social networking sites			✓		
Downloading video broadcasting e.g. Youtube	✓				
Uploading to video broadcast e.g. Youtube			✓		

Appendix 3

Incident involving students	**Teacher to use school behaviour policy to deal with**	**Refer to Student Progress Leader – Liaise with ESC as appropriate**	**Refer to HT, ESC, SLT, Police**	**Refer to technical support staff for action re security/filtering etc**
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/ inappropriate activities**).**		✓	✓	✓
Unauthorised use of non-educational sites during lessons	✓			✓
Unauthorised use of mobile phone/ digital camera/ other handheld device.	✓			
Unauthorised use of social networking/ instant messaging/ personal email	✓	✓		✓
Unauthorised downloading or uploading of files		✓		✓
Allowing others to access school network by sharing username and passwords		✓		✓
Attempting to access or accessing the school network, using another student's account		✓		✓
Attempting to access or accessing the school network, using the account of a member of staff		✓		✓
Corrupting or destroying the data of other users		✓		✓
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		✓		✓
Continued infringements of the above, following previous warnings or sanctions		✓	Community Police Officer referral	✓
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		✓		✓
Using proxy sites or other means to subvert the school's filtering system		✓		✓
Accidentally accessing offensive or pornographic material and failing to report the incident		✓		✓

The guidance in this policy should be implemented with cross reference to the Safeguarding, Anti-Bullying and Behaviour Policies. Note, attempts have been made to synchronise guidance and sanctions.

Appendix 4

Incidents involving members of staff	**Refer to the HT** ***See below**	**Refer to technical support staff for action re filtering, security etc**	**Referral to LADO** **Potential Disciplinary Action**
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable /inappropriate activities).	✓	✓	✓
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	✓		✓
Excessive or inappropriate personal use of the internet/social networking sites/ instant messaging/ personal email	✓	✓	✓
Unauthorised downloading or uploading of files	✓	✓	✓
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account.	✓	✓	✓
Careless use of personal data e.g. holding or transferring data in an insecure manner	✓		✓
Deliberate actions to breach data protection or network security rules	✓	✓	✓
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	✓	✓	✓
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	✓	✓	✓
Using personal email/ social networking/ instant messaging/ text messaging to carrying out digital communications with students/ pupils	✓	✓	✓
Actions which could compromise the staff member's professional standing	✓		✓
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	✓		✓
Using proxy sites or other means to subvert the school's filtering system	✓	✓	✓
Deliberately accessing or trying to access offensive or pornographic material	✓	✓	✓
Breaching copyright or licensing regulations	✓	✓	✓
Continued infringements of the above, following previous warnings or sanctions	✓		✓

***In event of breaches of policy by the Headteacher, refer to the Chair of IEB.**

Appendix 5

Acceptable Use Agreement (AUA) – Pupils and Parents/ Carers

St Hild's Church of England School promotes the use of technology in school as all pupils will need the skills and knowledge in whatever field of work they enter when they become an adult. We ensure that our school ICT network is robust and resilient and we do our upmost to ensure the safety of children when using it. It is important that pupils abide by the school rules when using technology in school and inform a member of staff immediately, if they become aware of any misuse.

This is the Acceptable User Agreement (AUA) for our school. It highlights the do's/don'ts of using all technology in school and shows how we want pupils to behave when using IT. Any misuse will result in pupils being temporarily banned from using the school network. In addition, the AUA covers the following legislation:

- Malicious Communications Act
- 1988 Data Protection Act 1998
- Computer Misuse Act 1990
- Communications Act 2003
- Sexual Offences Act 2003

Please read carefully and sign at the bottom to show you agree to these terms. If you do not sign and return this form you will not be able to use the IT systems in school.

For Pupils:

Using Technology in Schools

- I will only use school Internet, IT facilities and mobile technologies for educational purposes which follow the teachers' instructions. This includes email, video, messaging, video-conferencing, using software apps, social media, Internet, file-saving and printing.
- I will only use my mobile phone, mobile device or smartwatch in school when permission has been granted by a teacher. If permission is granted, I will use my mobile device in line with how I would use other technology in school.
- I will not look at or delete or amend other people's work or files.
- I will treat all IT equipment at school with respect and ensure the computer or mobile device is left in the state that I found it.

Security, Passwords & Copyright

- I will not install software on school IT facilities due to the risk of damage being caused by malware or viruses. I will ask an ICT technician(Dataspire) to install software if required.
- I will only install software apps on mobile devices when directed to by a teacher. I will only use school-related information when registering for an app.
- I will not share my network, Internet or any other school-related passwords.
- I will change my passwords when asked to and ensure that they have complexity e.g. Capital, lower case letters, numbers and symbols.
- I will only use my school-supplied email address for school-related activities.
- I will respect copyright when making use of images, videos or other media in my school work. I will use and attribute 'Creative Commons' material as taught in ICT/e-safety lessons.

- I will follow the school procedures when using removable media e.g. flash drives to ensure that I don't infect any machines.
- I will not look for ways to bypass the school filtering, monitoring or proxy service.
- I will not bypass the school filtering, monitoring or proxy service.

Online Behaviour & Safety

- I will make sure all my contact with other people at school is responsible. I will not cyber-bully pupils, teachers or other members of staff.
- I will be responsible and polite when I talk online to pupils, teachers and other people related to the school, both in school-time and outside school-time.
- I won't look for or look at unpleasant, unsuitable or extremist websites in school. I will check with a teacher if I think a website might be unsuitable.
- I won't give out my personal details, such as my name, address, school or phone number on the Internet.
- I won't meet people I've met on the Internet unless I have told my parents and they come with me.
- I won't upload or download any pictures, writing or films which might upset people online.
- I won't write unpleasant, rude or untrue comments online about pupils, teachers or other staff employed by the school.
- I won't share inappropriate images or videos of other pupils on the school network or personal devices.
- I am aware that everything I do on the computers at school is monitored and logged, and that the school can talk to my parents if a teacher is concerned about my online safety or my behaviour when using school computers.
- I will not look for, view, upload or download offensive, illegal, copyright-infringing or pornographic material. If I find such material on school IT equipment I will inform a teacher immediately.
- I understand that these rules are designed to keep me safe and that if they are not followed, sanctions may be applied and my parent/guardian may be contacted.

For parents/carers:

- I agree to support and uphold the principles of this agreement in relation to my child and their use of the Internet, at home and at school.
- I agree to uphold the principles of this agreement in relation to my own use of the Internet, when that use is related to the school, employees of the school and other students at the school.
- Images of pupils will only be taken, stored and used for school purposes in line with school policy. Images will only be used on the Internet or in the media with permission.

Signed - Pupil: _____

Pupil Name: _____

Signed - Parent/Guardian: _____

Date: _____

Appendix 6

Acceptable Use Agreement (AUA) – Staff

This AUA is an agreement between the school and every member of staff. This agreement is to cover the use of all school equipment, the use of the school's network and Internet and Unity access. If the school AUA is not adhered to, all access will be withdrawn and appropriate sanctions imposed. Therefore the AUA must be read carefully before any acceptance of the AUA.

Aims:

The aims of the Acceptable Use Agreement are:

- To allow staff to benefit from the ICT facilities on offer by the school.
- To provide staff with ICT resources to improve learning and teaching at St Hild's Church of England School.
- To give guidance on security, responsibilities and protection within the use of all ICT resources and equipment.
- To ensure the schools ICT network and infrastructure is protected against missus or attack.

Day to day use:

- Although the school's ICT is primarily under the Dataspire managed service, the use of any ICT equipment and the network is regularly monitored by key school senior staff. This is to ensure the systems are used in a responsible way and any outside threats are dealt with swiftly.
- All sections of the schools network, file structure and email system may need to be accessed at key intervals but will only be done so under full consultation by senior staff.
- All members of staff need to be aware of their responsibilities to data protection and the use of any files containing sensitive child information.
- Observe good computer etiquette and be respectful to all users of ICT equipment. Never undertake actions that will bring the school into disrepute, offend other members of staff or cause harassment to others.
- On public computers, please log off once finished and shut down computers at the end of the day.
- ICT equipment must not be used for any illegal or disreputable activity. This includes:

- Use of illegally obtained software, videos, music etc.
- Deliberate viewing of inappropriate materials either through the internet or from files on a computer / USB data stick / portable hard drive.
- All private USB data sticks / portable hard drives or devices that need to attach to St Hild's Church of England Schools ICT equipment must first be scanned by Dataspire personnel.
- Unauthorised copying of software or illegally downloading any files.
- All new software titles must be authorised and purchased by Senior staff in charge of ICT.
- All data will be regularly backed up by Dataspire that is saved in Staffshared. For all other saved work it is the responsibility of the individual teacher to make a back up of files.

Staff laptops / Ipads:

- Laptops / Ipads that are supplied to you by the school are the school's property and are on loan to you whilst employed at St Hild's Church of England School.
- No laptop is to be used outside of the school unless it has been updated with PGP encryption.
- Laptops / Ipads need to be used within the school at least once a month so updates can be performed by Dataspire.
- Laptops should never be left unattended outside of school.
- When transporting Laptops please ensure they are well protected, don't leave them in unattended cars unless they are securely concealed in the boot.
- When saving work on laptop it is your responsibility to save your work to the correct location. No back-up of data will be made on a laptop and lost data will not be recoverable.

Security:

- Dataspire ensure all equipment is safe and secure. All equipment has antivirus software, all equipment has software to check misuse, all laptops are encrypted and all sections of the network are password protected and only accessible to those who need access.
- As part of the managed service all passwords will need to be changed on a regular basis.
- Never allow others to know your password and never use any other account other than your own.
- Always either lock or log out of a computer if you are going to leave it unattended.
- Do not alter or change any security settings, they are there to protect you, your work and your resources.
- Be mindful of your surroundings when looking at sensitive information. Do not use your account in public places like internet cafes, bars etc.

Internet:

- You are expected to exercise professional conduct when accessing the web, making sure only sites appropriate for viewing at school are accessed.
- If you require a website to be unblocked please use the standard routes of communication with Dataspire

Mobile Phones:

- School mobile phones only should be used to contact parents/carers/pupils when on school business with pupils off site. Staff should not use personal mobile devices.
- Staff should not use personal mobile phones in school during working hours when in contact with children.

E mail:

Email should be used to communicate short essential information to individuals or groups. St.Hild's Church of England School subscribes to the principles outlined in the Hartlepool Borough Council Internet Policy (copy on Staff Shared drive in the folder Staff Handbook).

i) Unacceptable use of the School's e-mail facility and addresses includes:

- Using inappropriate language e.g. profanities
- Taking part in, or creating, chain letters
- Interfering with freedom of expression of others by 'jamming' or 'bombing' electronic mailboxes
- Intentionally initiating or forwarding viruses
- Including any material that is obscene, pornographic, sexually explicit, violent, defamatory, of a racist nature or which is intended to, harass, intimidate, abuse, threaten or bully another person
- Use of the School internal e-mail system to promote discussion on issues of school policy without the prior permission of the Headteacher or a member of the Leadership Team
- Use of the school internal e-mail system to argue a point or to resolve a problem/issue
- Actions which result in potentially large numbers of personal e-mails being received in a School e-mail address in a short space of time during working hours e.g. selling items on e-bay
- Printing off large volumes of personal e-mails and/or attachments using work printers unless arrangements have been made to reimburse the cost to the School
- Reading lengthy incoming personal e-mails and/or attachments during working hours
- Sending large documents to Global Groups. If you need to share large files this should always be done via the Staff Shared area
- Drafting and/or sending outgoing personal e-mails during working hours. Inappropriate use of Global Groups e.g., '**ALL STAFF'**.

ii) Acceptable use of the School's e-mail facility and addresses includes:

- Receiving small numbers of personal e-mails
- Printing off the occasional personal e-mail and/or attachment using work printers

- Opening and identifying an e-mail as being personal (once recognised as being personal the remainder of the e-mail should not be read during working hours unless it is very short)
- Reading lengthy incoming personal e-mails and/or attachments outside of working hours
- Drafting and/or sending outgoing personal e-mails and/or attachments outside of working hours
- Regularly doing routine 'housekeeping' - deleting redundant messages to prevent 'clogging up' the system.

E-mails that contain specific or confidential information about a pupil should be sent to members of staff on a strictly 'need-to-know' basis and should comply with the conditions outlined below.

Use an Auto-Signature

Users of St. Hild's Church of England School E-mail facilities are expected to use an auto-signature on all business e-mails intended for distribution. This should be in the following format:

- Name
- Job Title/Position
- Address
- Telephone Number
- Fax Number (If Applicable)
- E-mail Address

Managing E-mail Accounts

All users are responsible for the maintenance of their e-mail accounts, and should:

- Check accounts on a regular basis
- Acknowledge or respond to e-mail promptly
- Delete unwanted and unnecessary messages and any correspondence that may be needed should be archived on a regular basis

Arrangements for Leave

Employees intending to take leave of more than 5 days must ensure that in their absence, their School mailboxes are set up to:

- Ensure that their mail is forwarded to a colleagues mailbox (by prior arrangement) so that all incoming e-mails can be dealt with during their leave.

- Provide automated replies to senders advising of their absence and providing details of an alternative contact person if matters are urgent.

Contractual E-mails

- Unless authorised, (such as for placing orders with suppliers etc) do not send, forward, or reply to email messages or documents, which are or may be construed as contractually binding to the School.

Data Protection, Freedom of Information, evidence in court proceedings

- The Data Protection Act and Freedom of Information Act apply equally to e-mails and e-mails sent or received (including personal and work related e-mails) may need to be disclosed in court proceedings, even if they are subsequently deleted from mailboxes. Employees should bear this in mind when using e-mails.

I have read this document carefully. I understand that if I violate these rules and requirements, access to the schools network will be denied and I may be subject to disciplinary action. I also understand that additional action may be taken by the school in line with existing polices and, where appropriate, the police may be involved or other legal action taken.

Staff Name: _____

Staff Signature: _____Date: _____

Appendix 7

Acceptable Use Agreement (AUA) – Volunteers/adults

This AUA is an agreement between the school and the public. This agreement is to cover the use of all school equipment, the use of the schools network and Internet access. If the school's AUA is not adhered to, all access will be withdrawn and appropriate sanctions imposed. Therefore the AUA must be read carefully before any acceptance of the AUA.

Aims:

The aims of the Acceptable Use Agreement are:

- To allow the public to benefit from the ICT facilities on offer by the school.
- To provide the public with ICT resources.
- To give guidance on security, responsibilities and protection within the use of all ICT resources and equipment.
- To ensure the schools ICT network and infrastructure is protected against missus or attack.

Day to day use:

- Although the school's ICT is primarily under the Dataspire managed service, the use of any ICT equipment and the network is regularly monitored by key School senior staff. This is to ensure the systems are used in a responsible way and any outside threats are dealt with swiftly.
- All sections of the schools network, file structure and email system may need to be accessed at key intervals but will only be done so under full consultation by senior staff.

- Observe good computer etiquette and be respectful to all users of ICT equipment.
- On public computers, please log off once finished and shut down computers at the end of the day.
- ICT equipment must not be used for any illegal or disreputable activity. This includes:

- Use of illegally obtained software, videos, music etc.
- Deliberate viewing of inappropriate materials either through the internet or from files on a computer / USB data stick / portable hard drive.
- All private USB data sticks / portable hard drives or devices that need to attach to St Hild's Church of England ICT equipment must first be scanned by Dataspire personnel.
- Unauthorised copying of software or illegally downloading any files.
- All new software titles must be authorised and purchased by senior staff in charge of ICT.
- All data will be regularly backed up by Dataspire that is saved in the correct locations. For all other saved work it is the responsibility of the individual to make a back up of files.

Security:

- Dataspire ensure all equipment is safe and secure. All equipment has antivirus software, all equipment has Securus/Lightening software to check misuse, all laptops are encrypted and all sections of the network are password protected and only accessible to those who need access.
- Never allow others to know your password and never use any other account other than your own.
- Always either lock or log out of a computer if you are going to leave it unattended.
- Do not alter or change any security settings, they are there to protect you, your work and your resources.
- Be mindful of your surroundings when looking at sensitive information. Do not use your account in public places like internet cafes, bars etc.

Internet:

- You are expected to exercise professional conduct when accessing the web, making sure only sites appropriate for viewing at school are accessed.
- If you require a website to be unblocked please use the standard routes of communication with Dataspire

Name: _____

Signature: _____Date: _____

Appendix 8

Acceptable Use Agreement (AUA) – Governors

This AUA is an agreement between the school and members of the Governing Body. This agreement is to cover the use of all school equipment, the use of the schools network and Internet access. If the school's AUA is not adhered to, all access will be withdrawn and appropriate sanctions imposed. Therefore the AUA must be read carefully before any acceptance of the AUA.

Aims:

The aims of the Acceptable Use Agreement are:

- To allow the Governors to benefit from the ICT facilities on offer by the school.
- To provide the Governors with ICT resources.
- To give guidance on security, responsibilities and protection within the use of all ICT resources and equipment.
- To ensure the schools ICT network and infrastructure is protected against missus or attack.

Day to day use:

- Although the school's ICT is primarily under the Dataspire managed service, the use of any ICT equipment and the network is regularly monitored by key School senior staff. This is to ensure the systems are used in a responsible way and any outside threats are dealt with swiftly.
- All sections of the schools network, file structure and email system may need to be accessed at key intervals but will only be done so under full consultation by senior staff.

- On school computers, please log off once finished and shut down computers at the end of the session.
- ICT equipment must not be used for any illegal or disreputable activity. This includes: Use of illegally obtained software, videos, music etc. and deliberate viewing of inappropriate materials either through the internet or from files on a computer / usb data stick / portable hard drive.
- All private USB data sticks / portable hard drives or devices that need to attach to St Hild's Church of England ICT equipment must first be scanned by Dataspire personnel.
- All data will be regularly backed up by Dataspire that is saved in the correct locations. For all other saved work it is the responsibility of the individual Governor to make a back up of files.
- All materials relating to school business should be deleted at the end of term of office.

Security:

- Dataspire ensure all equipment is safe and secure. All equipment has antivirus software, all equipment has Securus/Lightening software to check misuse, all laptops are encrypted and all sections of the network are password protected and only accessible to those who need access.
- Never allow others to know your password and never use any other account other than your own.
- Always either lock or log out of a computer if you are going to leave it unattended.
- Do not alter or change any security settings, they are there to protect you, your work and your resources.

- Be mindful of your surroundings when looking at sensitive information. Do not use your account in public places like internet cafes, bars etc.

Internet:

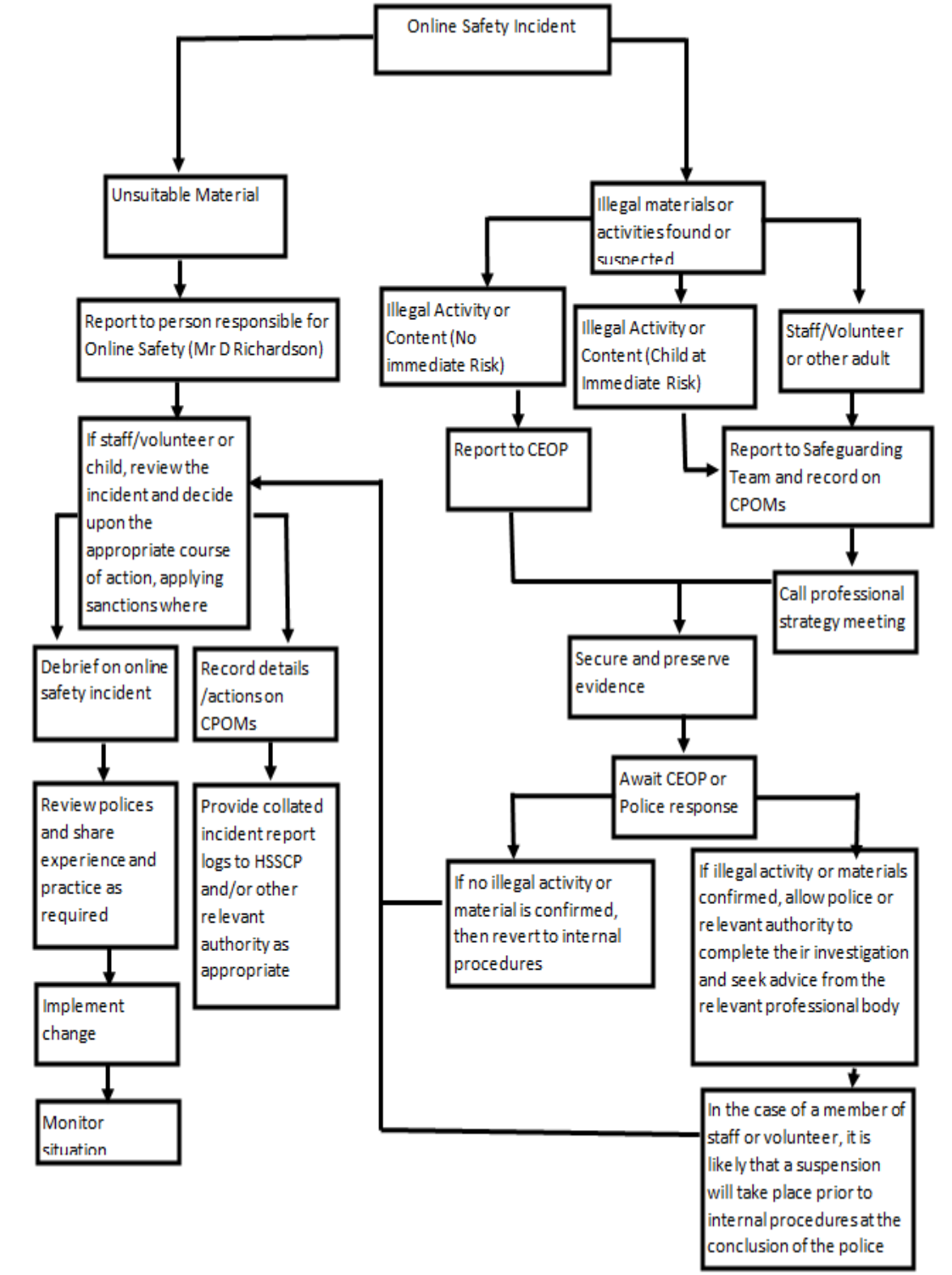
- You are expected to exercise professional conduct when accessing the web, making sure only sites appropriate for viewing at school are accessed.
- If you require a website to be unblocked please use the standard routes of communication with Dataspire

Name: _____

Signature:_____Date: _____

Appendix 9

Online Safety and misuse flow chart



Signed ……..(Headteacher)	
Signed …… (Chair of Governors)	**Next Review Date : February 2022 (Annual)**

Revision Date	Version	Status
Feb 2021	StHPol1-2	Agreed