St John's CE VA Primary School

Online Safety Policy
(E-Safety and Data Security Policy)

At St John's we are: Loved by God - Learning with Jesus - Living by the Spirit

1. Introduction

The St John's CEVA Primary School's online safety policy considers current and relevant issues, in a whole school context.

The term e-Safety has been replaced with 'Online Safety'. This fundamental change reflects a widening range of issues associated with technology and a user's access to content, contact with others and behavioural issues. The term Cyber bullying has also been replaced with 'Online Bullying'

National guidance suggests that it is essential for schools to take a leading role in e-safety. The Byron Review *'Safer Children in a Digital World'* stressed the role of schools and recommends:

"...delivering e-safety through the curriculum, providing teachers and the wider children's workforce with the skills and knowledge they need, reaching children and families through Extended Schools and taking steps to ensure that Ofsted holds the system to account on the quality of delivery in this area."

The development and expansion of the use of computing, and particularly of the internet, has transformed learning in schools in recent years. Children will need to develop high level computing skills, not only to maximise their potential use as a learning tool, but also to prepare themselves as lifelong learners and for future employment. There is a large body of evidence that recognises the benefits that technology can bring to teaching and learning. Schools have made a significant investment both financially and physically to ensure these technologies are available to all learners. The benefits are perceived to outweigh the risks. However, we must, through our policies, ensure that we meet our statutory obligations to ensure that our children are safe and are protected from potential harm, both within and outside school.

New technologies have become integral to the lives of children and young people in

today's society, both within schools and in their lives outside school.

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 / 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
- Online 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 online safety policy is used in conjunction with other school policies (e.g. behaviour, anti-bullying and safeguarding policies). 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.

2. Development, Monitoring & Review of this Policy

This online safety policy is developed through consultation with:

- School Online Safety Lead

- Designated Safeguarding Lead

- Headteacher
- Teachers
- Support Staff
- Computing Technician
- Governors
- Parents and Carers
- Pupils

Consultation with the school community will take place through the following:

- Staff meetings
- School Council (Pupil AUP)
- Curriculum committee meetings

3. Scope of the Policy

This policy applies to all members of the school community (including staff, pupils, volunteers, parents / carers and visitors) who have access to and are users of school computing capabilities, both in and out of the school.

The Education and Inspections Act 2006 empowers the headteacher to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site. This is pertinent to incidents of online bullying, or other online safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school.

The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the school behaviour policy.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where appropriate, inform parents / carers of incidents of inappropriate online safety behaviour that take place out of school.

Computing covers a wide range of resources, including web-based and mobile learning, and its use within society as a whole continues to evolve. Currently the internet technologies children and young people are using both inside and outside of the

classroom include:

- Websites
- Learning Platforms and Virtual Learning Environments
- E-mail and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality

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

At St John's CEVA Primary School we understand the responsibility to educate our pupils about online safety issues. We teach 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.

The online safety policy is written to closely aligned with the latest KCSiE document 2022 in which it states:
"It is essential that children are safeguarded from potentially harmful and inappropriate online material. An effective whole school and college approach to online safety empowers a school to protect and educate pupils, students, and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate."
The 4 key categories of risk that are included, considered and addressed are as follows:

"**content:** being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.

contact: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.

conduct: online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying, and

commerce: - risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group."

Everybody involved in the school has a responsibility to secure any sensitive information used in their day to day professional duties. In addition, school members not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

This policy and the Acceptable Use Policies for staff, governors, visitors and pupils (See Appendices 1 and 2) refer to any computing capabilities provided by the school or technologies owned by pupils and staff, but brought into school.

4. Roles and Responsibilities

4.1 Headteacher and Senior Leaders:

The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community. The day-to-day responsibility for online safety will be delegated to the Online Safety Lead.

The Headteacher and (at least) another member of the Senior Management Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (see 6.1 Flow chart - Dealing with Online safety incidents). The Headteacher and Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

4.2 Online Safety Lead:

The Online Safety Lead is responsible for:

• Taking day-to-day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents.

• Ensuring that all staff are aware of the procedures that need to be followed in the

event of an online safety incident taking place.

• Providing training and advice for staff

• Liaising with the Local Authority / relevant body

• Liaising with school technical staff

• Receiving reports of online safety incidents and creates a log of incidents to inform future online safety developments

• Meeting regularly with Online Safety Governor to discuss current issues, review incident logs and filtering / change control logs

• Attending relevant meeting / committee of Governors

• Reporting regularly to Senior Leadership Team

4.3 Computing Technician:

The Computing Technician is responsible for ensuring that:

• The school has an effective anti-virus programme in place.

• The school meets the online safety technical requirements outlined in the Acceptable Use Policy (See Appendices 1 and 2).

• The school is keeping up to date with online safety information in order to effectively carry out their online safety role and to inform and update others as relevant.

• Monitoring software and systems are implemented and updated as agreed in school policies.

4.4 Teaching and Support Staff:

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 Acceptable Use Policy (AUP) (See Appendix 2).

• They report any suspected misuse or problem to the Online Safety Lead and Headteacher for investigation.

• Digital communications with pupils (email, text, messaging, etc...) should be on a professional level and only carried out using official school systems.

• Online safety issues are embedded in all aspects of the curriculum and other school activities.

• Pupils understand and follow the school Online Safety Policy and Acceptable Use

Policy (See Appendix 1).

• Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

• They monitor the use of technology in lessons, extra-curricular and extended school activities

• They are aware of online safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement school policies with regard to these devices

• In lessons, where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

4.5 Designated Safeguarding Lead:

The designated Safeguarding Lead (DSL) should be trained in online safety issues and be aware of the potential for serious child protection issues to arise from:

• Sharing of personal data
• Access to illegal / inappropriate materials
• Inappropriate online contact with adults / strangers / children
• Potential or actual incidents of grooming
• Online bullying

4.6 Pupils:

All pupils are expected to:

• Use the school computing capabilities in accordance with the Acceptable Use Policy (AUP – Appendix 1). KS2 children will be expected to sign the policy before being given access to school systems. KS1 parents / carers will sign on behalf of their children.

• Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

• Understand the importance of reporting abuse, misuse or access to inappropriate materials.

• Where appropriate, know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on online bullying.

• Understand the importance of adopting good online safety practice when using

digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school.

4.7 Parents and Carers

Parents and 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 technology than their children. The school will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national or local online safety campaigns and literature. Parents and carers will be responsible for endorsing (by signature) the Acceptable Use Policy (AUP – Appendix 1).

4.8 Responsibilities of the Governing Body

As well as fulfilling their legal obligations, the governing body should also make sure that:

- all pupils make progress in achieving the expected educational outcomes;
- the subjects are well led, effectively managed and well planned;
- the quality of provision is subject to regular and effective self-evaluation;
- teaching is delivered in ways that are accessible to all pupils with SEND;
- clear information is provided for parents on the subject content and the right to request that their child is withdrawn;
- the subjects are resourced, staffed and timetabled in a way that ensures that the school can fulfil its legal obligations.
- the religious ethos of the school is maintained and developed.

5. Policy Statements

5.1 Education – pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety is therefore an essential part of the school's online safety provision. Children need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online Safety education will be provided in the following ways:

- A planned online safety programme is provided as part of Computing and PSHE lessons and should be regularly revisited – this will cover both the use of computing and new technologies in school and outside of school.
- Key online safety messages are reinforced as part of a planned programme of assemblies/ online safety week/ workshops and pastoral activities.
- The rising stars' online safety scheme of work will be used to deliver key online safety matters in each year group, from year 1 to year 6. It includes discrete online safety issues for each half term so a continuous curriculum is in place throughout the year.
- KS2 pupils are taught to be critically aware of the materials and content they access online and are guided to validate the accuracy of information.
- Pupils are helped to understand the need for the Acceptable Use Policy (AUP – Appendix 1) and encouraged to adopt safe and responsible use of technology and the internet both in school and outside of school.
- Pupils are being taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Rules for use of computing systems and the internet will be posted in all classrooms.
- Staff will act as good role models in their use of technology and the internet.

5.2 Education – parents and carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring and regulation of the children's online experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it.

The school will therefore seek to provide information and awareness to parents and carers through:

• Letters, newsletters, web site
• Parents evenings
• Parent information sessions

5.3 Training – Staff

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

• A planned programme of online safety training will be made available to staff.

• All new staff receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and Acceptable Use Policies (See Appendices 1 and 2).

• The Online Safety Coordinator will provide advice and guidance to individuals as required.

5.4 Training – Governors

Governors should take part in online safety training / awareness sessions, with particular importance for those who are members of any sub- committee e.g. health and safety / safeguarding. This may be offered in a number of ways:

• Attendance at training provided by the Local Authority / National Governors Association / or other relevant organisation.

• Participation in school training / information sessions for staff or parents.

5.5 Technical – infrastructure, filtering and monitoring

The school is responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

• School computing systems will be managed in ways that ensure that the school meets this Policy and guidance.

• There will be regular reviews of the safety and security of school computing systems.

• Servers, wireless systems and cabling must be securely located.

• All users will have clearly defined access rights to school computing systems.

• Pupils will use individual (or class logins where appropriate) to access the network.

• All users will be provided with a username and staff access will be through a password. Staff users will be required to change their password on a regular basis.

• The "master / administrator" passwords for the school computing systems, used by the Computing Technician (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 and Headteacher's locked file).

• Users will be made responsible for the security of their username and password must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.

• An agreed policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers visitors) onto any shared school digital storage (e.g. shared folders on server).

• Appropriate security measures are in place to protect the computing system and infrastructure from accidental or malicious attacks which might threaten the security of the school systems and data.

• Personal or sensitive data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

5.6 Bring Your Own Device (BYOD)

Unless approved by the Headteacher, the school does not allow the use of non-school devices on the computing systems / infrastructure of the school.

5.7 Curriculum

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages in the use of technology across the curriculum.

In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches. Where pupils are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.

Pupils are taught in all lessons to be critically aware of the materials / content they access online and be guided to validate the accuracy of information. Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

5.8 Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. The school will inform and educate users about these

risks and will implement policies to reduce the likelihood of the potential for harm.

Staff can take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. (See Data Protection Policy) If personal equipment has been used for such purposes then images should be transferred to the school network and deleted from the device as soon as possible. Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute. Pupils and staff must not take, use, share, publish or distribute images of others in school without their permission.

Photographs published on the school website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images. Pupils' full names will not be used anywhere on a website or blog. Written permission from parents or carers will be obtained before photographs of pupils are published on the school website as part of the agreement signed by parents when a child joins the school.

5.9 Data Protection

Personal data will be recorded, processed, transferred and made available in accordance with the Data Protection Act 1998, and from 25th May 2018 in accordance with the principles of the General Data Protection Regulation (GDPR). See Data Protection Policy.

5.10 Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. When using communication technologies, the school considers the following as good practice:

- The official school email service may be regarded as safe and secure.
- 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, text, messaging, etc...) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses or

public chat / social networking programmes must not be used for these communications.

Pupils are taught about email safety issues, such as the risks attached to the use of personal details. They are taught strategies to deal with inappropriate emails and are 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.

5.11 Unsuitable and 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 computing systems. Other activities e.g. Online 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. This policy restricts usage of the school computing systems as follows:

Usage	Restriction
Online gaming (educational)	Restricted at times for all users
Online gaming (non-educational)	Not acceptable
Online gambling	Not acceptable
Online shopping	Restricted at times for staff Not acceptable for non-staff
File sharing	Acceptable for staff only
Use of social media	Not acceptable
Use of messaging apps	Not acceptable
Use of video broadcasting, e.g. YouTube	Restricted at times for staff

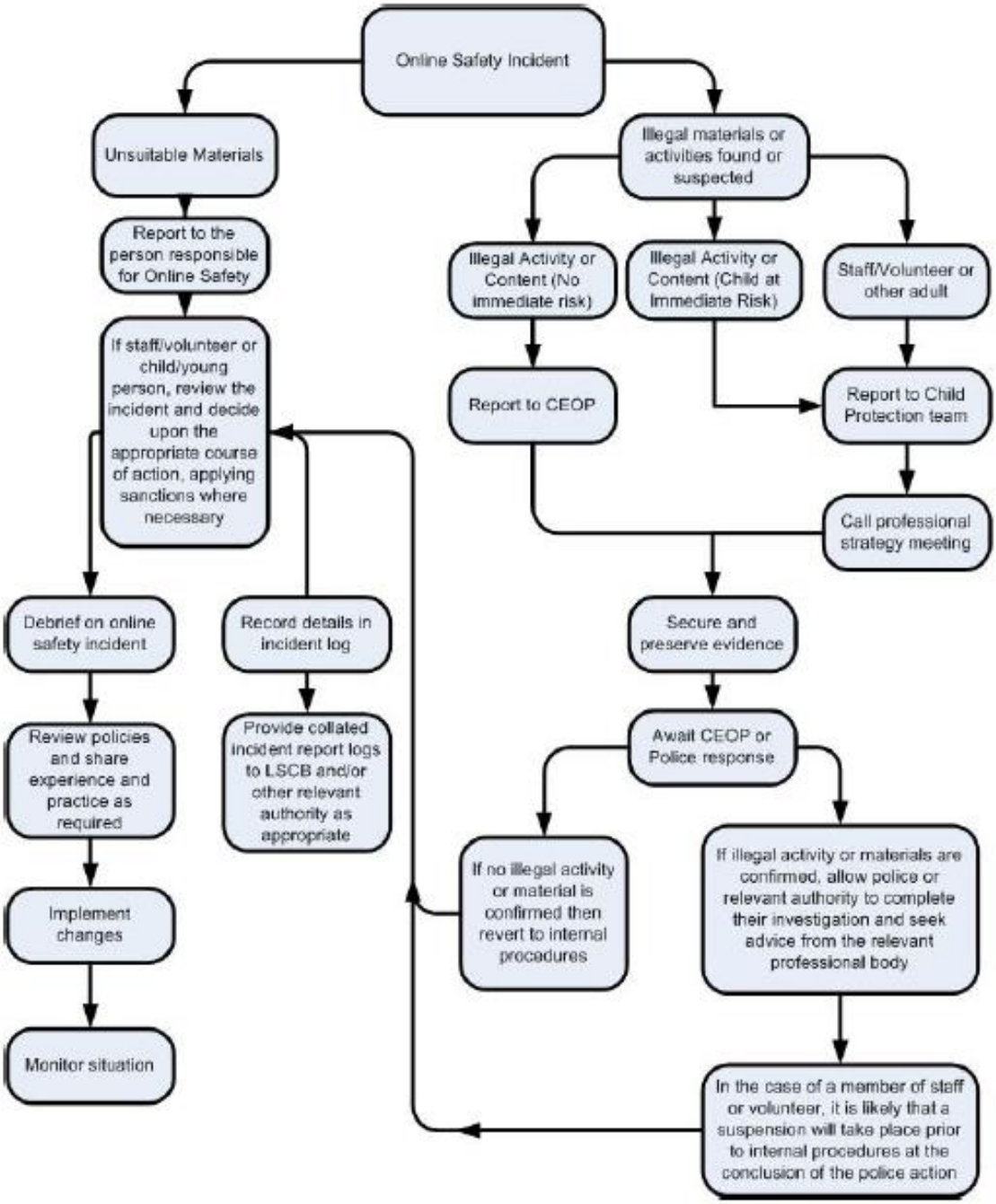
6. Responding to incidents of misuse illegal incidents

The following flowchart outlines the procedure to be followed when responding to incidents of misuse or illegal incidents.

Follow the right-hand side of the flow chart 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 and report immediately to the police.

6.1 Flow chart - Dealing with Online safety incident



The Online Safety Lead will keep a digital log of any incidents reported on the secure My Concerns software package.

7. Linked Policies

Due to the focus and purpose of this policy, there are also direct and intrinsic links to the following: St John's CE VA Primary School File:

- Behaviour and Discipline Policy
- Anti-Bullying Policy
- Safeguarding Policy
- Collective Worship Policy
- SMSC Policy
- RSE Policy
- Equalities Policy
- Science Policy
- RE Policy
- PE Policy
- SEN Policy

Please also refer to those named policies for more comprehensive information.

		Date
version	1.6	01.09.2021
Drafted by	Mr Dunne	12.11.2015
Reviewed by	Mr Dunne	07.03.2023
Approved by	Curriculum Committee	
Ratified by	Whole Governing Body	22.03.2023
Review period	1 year	
Date of review		March 2024

St John's CE VA Primary School

Appendix 1 Acceptable Use Policies (AUP) - Pupil

School Policy

New technologies are important in our lives, both within and outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. Children should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

• That our children will be responsible users and stay safe while using the internet and other.

• That school systems and users are protected from accidental or deliberate misuse.

• The school will try to ensure that children will have good access to computing capabilities to enhance their learning and will, in return, expect our children to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school computing systems in a responsible way, to ensure that there is no risk to my safety or to the safety of others.

For my own personal safety:

• I understand that the school will monitor my use of the computing systems, email and other digital communications.

• I will treat my username and password like my toothbrush – I will not share it, nor will I try to use any other person's username and password.

• I will be aware of "stranger danger", when I am communicating online.

• I will not share personal information about myself or others when online.

• I will immediately report anything that makes me feel uncomfortable to my teacher or an appropriate adult when I see it online.

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

• I will respect other people's work and property and will not change, copy or delete anyone else's work without their permission.

• I will be polite and responsible when I communicate with others

• I will not use pictures of anyone without their permission.

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 when I am out of school and where they involve other members of the school e.g. online bullying.

Please complete the sections below to show that you have read, understood and agree to these rules.

Pupil Acceptable Use Agreement Form

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

• I use the school computing systems and equipment both in and out of school.

• I use my own equipment out of school in a way that is related to me being a member of this school.

If you do not sign and return this agreement, access will not be granted to school computing systems.

Name of pupil: .....

Class: .....

*Signed: .....

Date: .....

For pupils in class R, 1 or 2, their parent / carer will sign on their behalf.

St John's CE VA Primary School

Appendix 2 Acceptable Use Policy (AUP) – Staff / Volunteer

School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

• That staff and volunteers will be responsible users and stay safe while using the internet and other technologies for educational, personal and recreational use.

• That school computing 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 computing systems 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 computing systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the computing systems and other users.

I recognise the value of the use of technology for enhancing learning and will ensure that pupils receive opportunities to gain from the use of technology. I will, where possible, educate the young people in my care in the safe use of technology and embed online safety in my work with young people.

For my professional and personal safety:

• I understand that the school will monitor my use of the computing systems, email

and other digital communications.

• I understand that the rules set out in this agreement also apply to use of school computing systems (e.g. laptops, email, VLE, etc...) out of school.

• I understand that the school computing systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.

• I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.

• I 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 computing systems:

• 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 and when personal equipment has been used for such purposes, images will be transferred to the school network and then deleted from the device as soon as possible.

• Where these images are published (e.g. on the school website) it will not be possible to identify by name, or other personal information, those who are featured.

• I will only communicate with pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner.

• I will not engage in any online activity that may compromise my professional responsibilities.

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

• When I use my personal devices (laptops / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti- virus software and are free from viruses.

• I will not use personal email addresses on the school computing systems unless given permission from the Headteacher or Online Safety Lead.

• I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.

• I will ensure that my data is regularly backed up, in accordance with relevant school policies.

• I will not try to upload, download or access any materials which are illegal 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 install or attempt to install (unless I have permission) 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 this policy. Where personal data is transferred outside the secure school network, it must be encrypted.

• I understand that data protection policy requires that any staff or pupil data, to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.

• I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

• 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 school:

• I understand that this Acceptable Use Policy applies not only to my work and use of school computing equipment in school, but also applies to my use of school computing systems and equipment out of school and my use of personal equipment in school 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, a warning, a suspension, referral to Governors and / or

the Local Authority and in the event of illegal activities the involvement of the police.

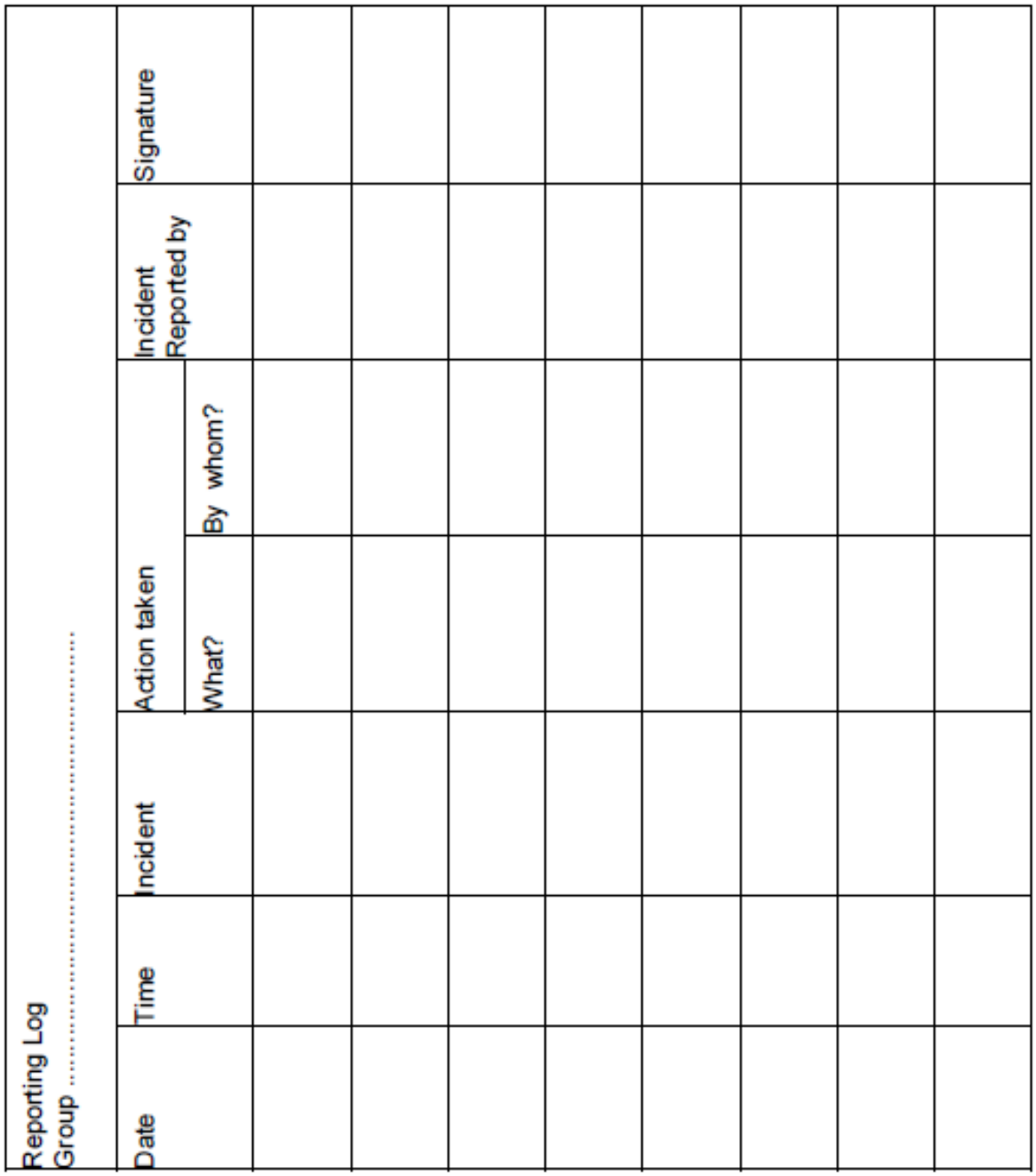
I have read and understand the above and agree to use the school computing systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Name of pupil: .....

Signed: ..... Date: .....

St John's CE VA Primary School

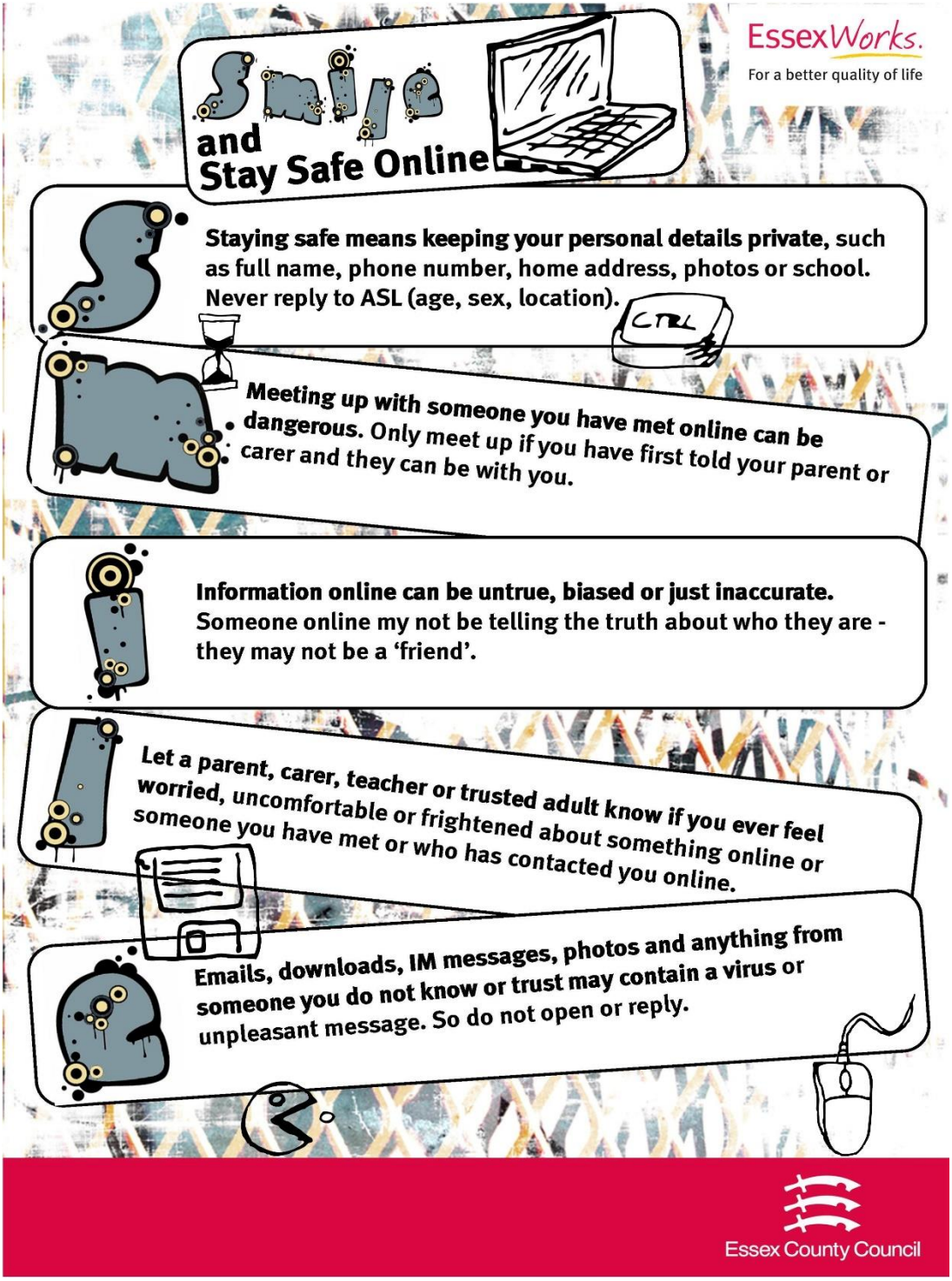
Appendix 3 Computing Reporting Log



St John's CE VA Primary School

Appendix 4 Online Safety Posters

Online safety guidelines to be displayed throughout the school.




Childnet International
www.childnet.com
Be smart on the internet
S
SAFE
Keep safe by being careful not to give out personal information – such as your full name, email address, phone number, home address, photos or school name – to people you are chatting with online.
M
MEETING
Meeting someone you have only been in touch with online can be dangerous. Only do so with your parents' or carers' permission and even then only when they can be present.
A
ACCEPTING
Accepting emails, IM messages, or opening files, pictures or texts from people you don't know or trust can lead to problems – they may contain viruses or nasty messages!
R
RELIABLE
Information you find on the internet may not be true, or someone online may be lying about who they are.
T
TELL
Tell your parent, carer or a trusted adult if someone or something makes you feel uncomfortable or worried, or if you or someone you know is being bullied online.
You can report online abuse to the police at www.thinkuknow.co.uk
THINK U KNOW
www.kidsmart.org.uk
KidSMART
Visit Childnet's Kidsmart website to play interactive games and test your online safety knowledge. You can also share your favourite websites and online safety tips by Joining Hands with people all around the world.