E-safety policy

Saffron Walden County High School

Date adopted or ratified;	January 2021
Last reviewed on:	
Next review due by:	

Contents

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

2. Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the Department's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

Maintained schools and academies that follow the National Curriculum.

The policy also takes into account the National Curriculum computing programmes of study.

This policy complies with our funding agreement and articles of association.

3. Roles and responsibilities

3.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3)

3.2 The headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The designated safeguarding lead

Details of the school's DSL and deputies are set out in our child protection and safeguarding policy as well relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety (appendix 4 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board

This list is not intended to be exhaustive.

3.4 The ICT manager

The ICT manager is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a monthly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy

- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2)

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent factsheet – Childnet International

3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 3).

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum:

National Curriculum computing programmes of study.

From September 2020 **all** schools will have to teach:

- Relationships education and health education in primary schools
- Relationships and sex education and health education in secondary schools

In **Key Stage 3**, pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns

Pupils in **Key Stage 4** will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

*By the **end of secondary school**, they will know:*

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours

At Saffron Walden County High school, we understand the responsibility to educate our students on e-safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the Internet and related technologies, in and beyond the context of the classroom.

Schools hold personal data on learners, staff and other people to help them conduct their dayto-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in media coverage, and potentially damage the reputation of the school. This can make it more difficult for your school to use technology to benefit learners.

Everybody in the school has a shared responsibility to secure any sensitive information used in

their day to day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them. Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors and students) are inclusive of both fixed and mobile Internet; technologies provided by the school (such as PCs, laptops, personal digital assistants (PDAs), tablets, webcams, whiteboards, voting systems, digital video equipment, etc.); and technologies owned by students and staff, but brought onto school premises (such as laptops, mobile phones, camera phones, PDAs and portable media players, etc.).

5. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents.

Online safety will also be covered during parents' evenings.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers/form teachers will discuss cyber-bullying with their tutor groups, and the issue will be addressed in assemblies.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

7. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1-3). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1, 2 and 3.

8. Pupils using mobile devices in school

These should not be brought into school; if they are seen or heard on school premises they will be confiscated. They will be taken by staff to the main office for safekeeping.

If it is the first confiscation for that academic year the item can be collected at the end of the day.

If it is not the first confiscation for that academic year the item will be kept in school and will be returned at the end of the following day upon production of a letter from parents requesting return of the item.

If Mobile devices are required for educational purposes, please see appendix 8.

9. Staff using work devices outside school

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 3.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted.

If staff have any concerns over the security of their device, they must seek advice from the ICT manager.

Work devices must be used solely for work activities.

10. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on student acceptable use agreement. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures/staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

The DSL and deputy DSL will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 11.

This policy will be regularly reviewed following recommended guidelines. At every review, the policy will be shared with the governing board.

13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Complaints procedure

Appendix 1: Acceptable Use Agreement: Student - Secondary

Secondary Student Acceptable Use - Agreement / E-Safety Rules

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

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

For my own personal safety:

- I understand that the school will monitor my use of systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will be aware of the risks when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc.)
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

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

- I understand that the school systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- I will not try (unless I have permission) to make large downloads or uploads that might take up Internet capacity and prevent other users from being able to carry out their work.
- I will not use the school systems or devices for on-line gaming, on-line gambling, Internet shopping, file sharing, or video broadcasting (e.g. YouTube), unless I have permission of a member of staff to do so.

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

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

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

- I will only use my own personal devices (mobile phones / USB devices/ wearable technology etc.) in school if I have permission or in the Sixth Form as set out in the BYOD policy. I understand that, if I do use my own devices in the school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however

Dear Parent/ Carer,

ICT including the Internet, learning platforms, e-mail and mobile technologies have become an important part of learning in our school. We expect all students to be safe and responsible when using any ICT. It is essential that students are aware of E-Safety and know how to stay safe when using any ICT.

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

Students are also expected to read and discuss this agreement with their parent or carer and then to sign and follow the terms of the agreement. Any concerns or explanation can be discussed with their form teacher or Mrs Vanderpere-Brown, SWCHS E-Safety Co-ordinator.

Students: by signing you agree to follow these guidelines when:

- Using the school systems and devices (both in and out of school).
- Using your own devices in the school (when allowed) e.g. mobile phones, wearable technology, USB devices, cameras etc.
- I use my own equipment out of the school / academy in a way that is related to me being a member of this school / academy e.g. communicating with other members of the school, accessing school email, VLE, website etc.

Parents: by signing this agreement you also agree to:

- Support the school approach to on-line safety and not deliberately upload or add any images, sounds or text that could upset or offend any member of the school community

This Acceptable Use Agreement is a summary of our E-Safety Policy which is available in full via our publications scheme on our website.

Please return this form to school for filing via your child's form tutor.

Student and Parent/ carer signature

We have discussed this document and …….....(Student name) agrees to follow the E-Safety rules and to support the safe and responsible use of ICT at Saffron Walden County High School.

Parent/ Carer Signature ……..…….……

Student Signature…….

Form …… Date ……

Appendix 2: Acceptable Use Agreement: Staff, Governors and Visitors

Staff, Governor and Visitor
Acceptable Use Agreement / Code of Conduct

ICT (including data) and the related technologies such as e-mail, the Internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with Katie Vanderpere-Brown, SWCH school E-Safety Co-ordinator or Jennifer Sims, Safeguarding Officer. This Acceptable Use Agreement (for all staff, governors, visitors and students) is inclusive of both fixed and mobile Internet; technologies provided by the school (such as PCs, laptops, personal digital assistants (PDAs), tablets, webcams, whiteboards, voting systems, digital video equipment, etc.); and technologies owned by students and staff, but brought onto school premises (such as laptops, mobile phones, camera phones, PDAs and portable media players, etc.).

- ✓ I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- ✓ I will comply with the ICT system security and not disclose any passwords provided to me by the school.
- ✓ I will ensure that all electronic communications with students and staff are compatible with my professional role (see staff conduct policy for guidelines).
- ✓ I will not give out my own personal details, such as mobile phone number, personal e-mail address and social networking identities to students.
- ✓ I will only use the approved, secure e-mail system(s) for any school business.
- ✓ I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body. Personal or sensitive data taken off site must be encrypted.
- ✓ I will not install any hardware of software without permission of Tariq Nabi.
- ✓ I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- ✓ Images and video of students and/ or staff will only be taken, stored and used for professional purposes inline with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher.(See also Star appendix of E-Safety Policy)
- ✓ I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Headteacher.
- ✓ I will respect copyright and intellectual property rights.
- ✓ I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- ✓ I will support and promote the school's E-Safety and Data Security policies and help students to be safe and responsible in their use of ICT and related technologies.
- ✓ I understand this forms part of the terms and conditions set out in my contract of employment.

This Acceptable Use Agreement is a summary of our E-Safety Policy which is available in full via our publications scheme on our website.

User Signature
I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school

Signature …… Date ……

Appendix 3: Curriculum E-Safety

Computing:

- In year 7 the students are taught in term 3 what to do in case of inappropriate conduct with people online or suspicious activity. The main guidelines from the thinkuknow website will be covered for that age range. The dangers of things being in the public domain and giving out content that is personal, cyber bullying, e stalking. They will be creating an informative video on the topic for a younger audience.

- They will also be told about CEOP and shown how to fill in the form on their website.

- Later in year 8 they will cover the laws associated with the use of computers within the UK.

- Throughout all Computing courses, students are taught how to search for relevant information on the web and are also taught the importance of ensuring that they do not plagiarise or breech copy write laws.

- UK laws with regard to Computing are revisited in most year groups for those who take opt to study Computing as a GCSE or A level subject.

- E-safety is also covered in schools PSHE programme in year 7

Appendix 4 : NOT IN USE

Appendix 5: BYOD Policy – Sixth Form

Purpose: For some time now students in the sixth form have been using their devices in school and connecting to the school network. This purpose of this policy is to clearly document our schools policy for BYOD in the sixth form, and formalise the use of the school network by individuals.

Audience: All students that access the school's Wi-Fi networks, and/or use electronic devices to complete school work or self-directed learning or recreational activities while in school.

Definition: BYOD, an acronym for Bring Your Own Device, refers to any student-owned electronic device used to complete coursework, classwork, and other work in the process of learning a curriculum subject in a given content area.

What You Can Use: A device is prohibited if it is or otherwise potentially hazardous to the health of users, staff, or students. This means laptops, Android phones, iPhones, iPads, Google Tablets, Windows Phones, and other smartphones and tablets are approved if they allow you to complete your work without burdening school resources (see consequences), or the academic performance of your peers. Please note, you may only charge devices using approved chargers supplied by the manufacturer. No other alternatives can be permitted on the school premises.

When in Doubt, Ask: If you are unsure about whether a device is permitted in a lesson ask your teacher right away and ask if you're unsure about a resource, network, app, or any related device use. We want you to benefit academically from the use of your device without damaging your device, or getting yourself in trouble. When in doubt, ask.

Viruses & Malware: Device security is the responsibility of the owner. Any device that threatens that security of your device, or the software and hardware around you needs to be turned off and/or otherwise corrected.

Other Risks: Device theft, password security, damage from environment hazards and dropping, and interference from nearby devices are your responsibility to prevent, recognise, and/or correct. SWCHS network support department is not responsible for maintaining or troubleshooting your devices. The school does not provide insurance for your device, you bring it on to school grounds at your own risk.

Connection: All students will use the provided SSID and password to gain access to the wireless network and the Internet. The school does not guarantee connectivity or the quality of the connection.

Digital Citizenship: One definition of digital citizenship *is "the* self-monitored *habits that* sustain and improve *the digital communities* you enjoy or depend on." Keep this in mind every time you send a text, update a social media profile, share a selfie, or recommend a resource to a friend, at school or

at home. Your digital actions and behaviour are not only permanent, but deeply impact those around you, even if it's not always immediately apparent how.

Think about how the use of your device might impact on a classroom environment. Approved devices must be in silent mode while in school unless otherwise allowed by a teacher. Headphones may be used only with a teacher's permission. You must not have your device out outside of the sixth form area including the front of school and school corridors.

Devices may not be used to cheat on classwork, coursework, or tests or for non-instructional purposes (such as making personal phone calls and text messaging). You may not use devices to record, transmit, or post photographic images or video of a person or persons in school during school hours or during school activities, unless otherwise explicitly allowed by a teacher.

Devices may only be used to access computer files on Internet sites which are relevant to the classroom curriculum (see consequences).

Training: Training is not provided for use of individual devices, apps, or platforms. One of the goals of BYOD is for you to use a device that you're comfortable with and accustomed to using under a variety of circumstances.

Bad Decisions: Any device use outside of the documented curriculum goals of a given classroom is prohibited, and in some cases punishable by law. Disrespectful communication, cyberbullying, spamming, sexting, copyright infringement, trolling, circumventing school filters or related device monitoring, and other abuses of technology will be documented, possibly leading to the loss of BYOD privileges, and enforcement by relevant law agencies.

This document does not replace the User Agreement for Electronic Equipment and Internet Use that your parents consented to, and signed on your behalf when you joined SWCHS. Please ensure you are familiar with the terms in the agreement. If you would like a copy, please contact Mrs Vanderpere-Brown.

Consequences: You have a choice to follow the above guidelines, or to not follow the above guidelines. You have the choice to make good decisions, or not, to find "holes" in our policy or not, and to demonstrate digital citizenship or not.

- Should you choose to misuse your device in a lesson environment, a teacher has the right to revoke your permission to use it in a classroom.

- Bandwidth is an important resource to all members of our school community and should be used for learning purposes only. Should you choose to abuse your access to the schools network connection, you will have your bandwidth restricted, or in extreme cases access to the network will be blocked for your device. For example, you should not be streaming media for non-academic purposes (YouTube, NetFlix, Spotify).

- In the event of this happening any attempt to ‘get round’ restrictions (such as changing the MAC address on your device) will be considered a serious breach of trust that will require the involvement of the Director of Sixth Form.

Contact: Mr P. Singh psingh@swchs.net

Publication of Policy: This policy will be posted publicly at the school, shared on the school website, and supplied on request.

Appendix 6: SWCHS Twitter Guidance for Students

Principles

1. Use of Twitter is for the broadcasting of:

    a. educational resources

    b. information relevant to your academic career at SWCHS

2. Use of the SWCHS Twitter accounts is a teaching & learning activity and when using them you should at all times conduct yourself as though you were in school

Following a school Twitter account

1. All school account names will have “SWCHS” at the start (e.g. SWCHSMaths)

2. If unsure of the relevant account, ask your subject teacher to locate it for you

Specific Use

1. Once you have your own Twitter account, you are able to ‘follow’ any school Twitter account

2. Searching for ‘hashtagged’ conversations is a good way of finding specific Tweets that are relevant to you. Your teacher will let you know which hashtags they are using

3. Do not send direct messages to your teachers via Twitter. You should use your school email account or speak to them in person

4. **Your account is your responsibility.** Teachers will not browse, follow or tweet directly to your individual accounts, but you should still think carefully about what you tweet and what impression you give to other people using Twitter

If you are concerned about anything you see or receive on Twitter, please speak to your tutor or to any member of staff

Appendix 7: SWCHS Twitter Guidance for Staff

Principles:

- Use of Twitter is for the broadcasting of:
    - educational resources
    - information relevant to students' academic career at SWCHS
- Use of Twitter is a teaching & learning activity and as such will be conducted **solely** in the manner befitting a professional student-teacher relationship
- Twitter is for use with students aged 13 & over, therefore **accounts can only be used in Years 9-13.**

Accounts:

- All account names are to be prefaced with "SWCHS" (e.g. SWCHSMaths)
- All login details are to be sent to ICT Support to be kept in a central register
- Each Twitter Account **MUST** be monitored by more than one member of staff

Specific Use:

- Tweets are to be open broadcasts, available to be followed by anyone.
- Tweets may be tagged in order to differentiate the target audience
- Staff are not permitted to browse, follow or tweet to students' Twitter accounts
- Staff are not permitted to follow the school Twitter feeds using their own personal Twitter account
- Direct messaging between staff and students is not permitted
- Tweets are to be appropriate for classroom use and as such conform to school policies and procedures
- Before sending a tweet, staff accept responsibility for checking the content of the tweets (including links and retweets) for appropriate language and content

Appendix 8: BYOD Policy Years 7-11

Current school rules state that students in year 7-11 are not permitted to bring a mobile phone, tablet or other device to school.

However, in approved circumstances that are proven to be educationally beneficial staff can follow the following policy:

1. Seek approval for the proposed activity from AC and put request in writing to E-Safety Co-ordinator including a draft of parental letter. Await approval.

2. Seek written permission from parents using the letter template below

3. Plan activity carefully with due consideration to the e-safety policy guidance

4. Review usage and report outcomes to E-Safety Co-ordinator

Dear Parent/ Carer,

(Introductory paragraph including activity and rationale)

I am therefore asking for your permission to allow (name) to bring in a device for the specific purpose mentioned above. (Name) should still adhere to the normal rules regarding mobile devices in all other lessons and when on the school site.

Please be aware that by giving your permission you are agreeing to the rules set out in the Sixth Form BYOD policy on use (available on school website and within school safety policy). In particular:

“Device theft, password security, damage from environment hazards and dropping, and interference from nearby devices are the student’s responsibility to prevent, recognise, and/or correct. SWCHS network support department is not responsible for maintaining or troubleshooting student’s devices. The school does not provide insurance for student’s personal devices, they bring them on to school grounds at their own risk.”

Student’s are required to access the Internet through the school provided SSID only. Mobile data should be switched off on any device whilst it is being used for the activity. This is to ensure that students are subject to normal filtering of explicit and inappropriate content.

Contact: Mr P. Singh psingh@swchs.net

Publication of Policy: This policy will be posted publicly at the school, shared on the school website, and supplied on request.

Appendix 9: E-Safety Group Terms of Reference

Purpose:

To provide a consultative group that has wide representation from the school and community, with responsibility for issues regarding e-safety and the monitoring the e-safety policy including the impact of initiatives. Depending on the size or structure of the school this group may be part of the safeguarding group. The group will also be responsible for regular reporting to the Full Governing Body.

Membership:

The e-safety group will seek to include representation from all stakeholders.

The composition of the group should include:

- SLT member/s
- Child Protection/Safeguarding officer
- Teaching staff member
- Support staff member
- E-safety coordinator (not ICT coordinator by default)
- Governor
- Parent / Carer
- ICT Technical Support staff
- Community users (where appropriate)
- Digital Leaders (Student / pupil representation – for advice and feedback. Student / pupil voice is essential in the make up of the e-safety group, but students / pupils would only be expected to take part in group meetings where deemed relevant.)

Other people may be invited to attend the meetings at the request of the Chairperson on behalf of the group to provide advice and assistance where necessary.

Group members must declare a conflict of interest if any incidents being discussed directly involve themselves or members of their families.

Group members must be aware that many issues discussed by this group could be of a sensitive or confidential nature.

When individual members feel uncomfortable about what is being discussed they should be allowed to leave the meeting with steps being made by the other members to allow for these sensitivities.

Chairperson:

The Group should select a suitable Chairperson from within the group. Their responsibilities include:

- Scheduling meetings and notifying group members;
- Inviting other people to attend meetings when required by the group;
- Guiding the meeting according to the agenda and time available;
- Ensuring all discussion items end with a decision, action or definite outcome;
- Making sure that notes are taken at the meetings and that these with any action points are distributed as necessary

Duration of meetings:

Meetings shall be held termly for a period of no more than one hour. A special or extraordinary meeting may be called when and if deemed necessary.

Functions:

These are to assist the E-safety Co-ordinator (or other relevant person) with the following:

- To keep up to date with new developments in the area of e-safety
- To (at least) annually review and develop the e-safety policy in line with new technologies and incidents
- To monitor the delivery and impact of the e-safety policy
- To monitor the log of reported e-safety incidents (anonymous) to inform future areas of teaching / learning / training.

To co-ordinate consultation with the whole school community to ensure stakeholders are up to date with information, training and/or developments in the area of e-safety. This could be carried out through:

- Staff meetings
- Student / pupil forums (for advice and feedback)
- Governors meetings
- Surveys/questionnaires for students / pupils, parents / carers and staff
- Parents evenings
- Website/VLE/Newsletters
- E-safety events
- Internet Safety Day (annually held on the second Tuesday in February)
- Other methods
- To ensure that monitoring is carried out of Internet sites used across the school
- To monitor filtering / change control logs (e.g. requests for blocking / unblocking sites).

- To monitor the safe use of data across the [school]
- To monitor incidents involving cyberbullying for staff and pupils

Amendments:

The terms of reference shall be reviewed annually from the date of approval. They may be altered to meet the current needs of all group members, by agreement of the majority.

Appendix 10 : Further Reading

UK Safer Internet Centre:

Safer Internet Centre -

South West Grid for Learning

Childnet

Professionals Online Safety Helpline

Internet Watch Foundation

CEOP:

http://ceop.police.uk/ ThinkUKnow

Others:

INSAFE - http://www.saferinternet.org/ww/en/pub/insafe/index.htm

UK Council for Child Internet Safety (UKCCIS) www.education.gov.uk/ukccis

Netsmartz http://www.netsmartz.org/index.aspx

Support for Schools:

Specialist help and support SWGfL BOOST

Cyberbullying:

Scottish Anti-Bullying Service, Respectme - http://www.respectme.org.uk/

Scottish Government Better relationships, better learning, better behaviour

DCSF - Cyberbullying guidance

DfE – Preventing & Tackling Bullying – Advice to school leaders, staff and Governing Bodies

Anti-Bullying Network - http://www.antibullying.net/cyberbullying1.htm

Cyberbullying.org - http://www.cyberbullying.org/

Social Networking:

Digizen – Social Networking

SWGfL - Facebook - Managing risk for staff and volunteers working with children and young people

Connectsafely Parents Guide to Facebook

Facebook Guide for Educators

Curriculum:

SWGfL Digital Literacy & Citizenship curriculum

Glow - http://www.educationscotland.gov.uk/usingglowandict/

Alberta, Canada - digital citizenship policy development guide.pdf

Teach Today – www.teachtoday.eu/

Insafe - Education Resources

Somerset - e-Sense materials for schools

Mobile Devices / BYOD:

Cloudlearn Report Effective practice for schools moving to end locking and blocking

NEN - Guidance Note - BYOD

Data Protection:

Information Commissioners Office:

Your rights to your information – Resources for Schools - ICO

ICO pages for young people

Guide to Data Protection Act - Information Commissioners Office

Guide to the Freedom of Information Act - Information Commissioners Office

ICO guidance on the Freedom of Information Model Publication Scheme

ICO Freedom of Information Model Publication Scheme Template for schools (England)

ICO - Guidance we gave to schools - September 2012 (England)

ICO Guidance on Bring Your Own Device

ICO Guidance on Cloud Hosted Services

Information Commissioners Office good practice note on taking photos in schools

ICO Guidance Data Protection Practical Guide to IT Security

ICO – Think Privacy Toolkit

ICO – Personal Information Online – Code of Practice

ICO – Access Aware Toolkit

ICO Subject Access Code of Practice

ICO – Guidance on Data Security Breach Management

SWGfL - Guidance for Schools on Cloud Hosted Services

LGfL - Data Handling Compliance Check List

Somerset - Flowchart on Storage of Personal Data

NEN - Guidance Note - Protecting School Data

Professional Standards / Staff Training:

DfE - Safer Working Practice for Adults who Work with Children and Young People

Kent - Safer Practice with Technology

Childnet / TDA - Social Networking - a guide for trainee teachers & NQTs

Childnet / TDA - Teachers and Technology - a checklist for trainee teachers & NQTs

UK Safer Internet Centre Professionals Online Safety Helpline

Infrastructure / Technical Support:

NEN - Guidance Note - esecurity

Working with parents and carers:

SWGfL / Common Sense Media Digital Literacy & Citizenship Curriculum

SWGfL BOOST Presentations - parents presentation

Connect Safely - a Parents Guide to Facebook

Vodafone Digital Parents Magazine

Childnet Webpages for Parents & Carers

DirectGov - Internet Safety for parents

Get Safe Online - resources for parents

Teach Today - resources for parents workshops / education

The Digital Universe of Your Children - animated videos for parents (Insafe)

Cerebra - Learning Disabilities, Autism and Internet Safety - a Parents' Guide

Insafe - A guide for parents - education and the new media

The Cybersmile Foundation (cyberbullying) - advice for parents

Research:

EU Kids on Line Report - "Risks and Safety on the Internet" - January 2011

Appendix 11: Forms and Templates

Record of reviewing devices / Internet sites (responding to incidents of misuse):

Group Date Reason for investigation

Details of first reviewing person

Name
Position Signature

Details of second reviewing person

Name
Position Signature

Name and location of computer used for review (for web sites):

Web site(s) address / device:	**Reason for concern:**

Conclusion and Action proposed or taken:

Template Reporting Log:

Reporting Log Group ……	Date	Time	Incident	Action taken		Incident Reported by	Signature
				What?	By whom?		