WELLSWAY SCHOOL

# Online Safety and Social Media Policy

**Adopted by the Local Governing Body:**

**December 2009**

**Revised March 2017**

**Date of Next Review March 2018**

# Contents

# 1. Aims and scope

Wellsway School believes that online safety (e-Safety) is an essential element of safeguarding children and adults in the digital world, when using technology such as computers, tablets, mobile phones or games consoles.

Wellsway School identifies that the internet and information communication technologies are an important part of everyday life, so children must be supported to be able to learn how to develop strategies to manage and respond to risk and be empowered to build resilience online.

Wellsway School has a duty to provide the community with quality internet access to raise education standards, promote achievement, support professional work of staff and enhance management functions.

The purpose of Wellsway School online safety policy is to:

- Clearly identify the key principles expected of all members of the community with regards to the safe and responsible use of technology to ensure that Wellsway School is a safe and secure environment.
- Safeguard and protect all members of Wellsway School's community online.
- Raise awareness with all members of Wellsway School's community regarding the potential risks as well as benefits of technology.
- To enable all staff to work safely and responsibly, to role model positive behaviour online and be aware of the need to manage their own standards and practice when using technology.
- Identify clear procedures to use when responding to online safety concerns that are known by all members of the community.

The Wellsway School Online Safety Policy (WSOSP) applies to all staff including the local governing body, teachers, support staff, external contractors , visitors, volunteers and other individuals who work for or provide services on behalf of the school (collectively referred to as 'staff' in this policy) as well as students and parents/carers.

The WSOSP applies to all access to the internet and use of information communication devices, including personal devices, or where students, staff or other individuals have been provided with school issued devices for use off-site, such as a work laptops, tablets or mobile phones.

The WSOSP must be read in conjunction with other relevant school policies including (but not limited to) safeguarding and child protection, anti-bullying, behaviour for learning, code of conduct, acceptable use, data protection, home-school agreement and relevant curriculum policies including Personal Social and Health Education (PSHE) and Sex and Relationships Education (SRE).

P Comber
Assistant Principal

# 2. Policies and Practices

## 2.1 Writing and reviewing the WSOSP

The WSOSP is annually reviewed as part of the School Development Plan.

The WSOSP should be read in conjunction with other relevant policies.

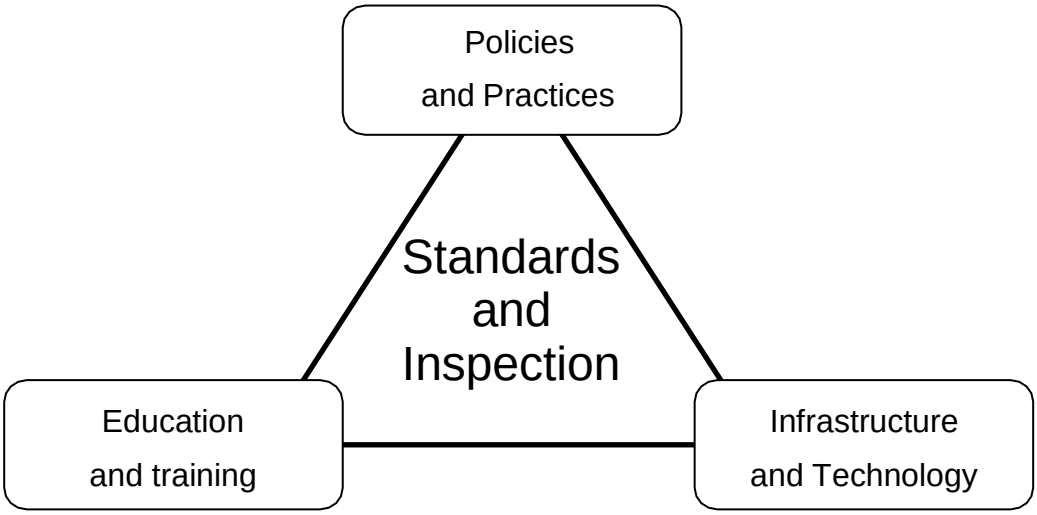
- WMAT Policy for managing allegation of abuse against staff
- WMAT Code of Conduct
- WMAT Whistleblowing Policy
- Wellsway School Behaviour for Learning Policy
- Wellsway School Anti-bullying Policy
- Wellsway School PHSE Policy

All action is taken in line with the following legislation/guidance:

- South West Child Protection Procedures (SWCPP)
- The Children Act 1989 and 2004
- The Children and Families Act 2014
- The Serious Crime Act 2015
- The Sex Offenders Act 2003
- Section 175 Children Act 2002
- The Education (Health Standards) (England) Regulations 2003
- The Education (Pupil Referral Units) (Application of Enactments) (England) Regulations 2007 as amended by SI 2010/1919, SI 2012/1201, SI 2012/1825, SI 2012/3158
- The School Staffing (England) Regulations 2009 as amended by SI 2012/1740 and SI 2013/1940
- The Education (Non-Maintained Special Schools) (England) Regulations 2011 as amended by SI 2015/387
- The Education (School Teachers' Appraisal) (England) Regulations 2012
- Computer Misuse Act 1990
- Data Protection Act 1998
- Freedom of Information Act 2000
- Communications Act 2003
- Malicious Communications Act 1988
- Regulation of Investigatory Powers Act 2000
- Trade Marks Act 1994
- Copyright Design and Patents Act 1988
- Telecommunications Act 1984
- Racial and Religious Hatred Act 2006
- Protection from Harassment Act 1997

- Criminal Justice and Immigration Act 2008
- Public Order Act 1986
- Obscene Publications Act 1959 and 1964
- Human Rights Act 1998
- The Education and Inspections Act 2006 and 2011
- The Protection of Freedoms Act 2012
- The School Information Regulations 2012
- The Counter Terrorism and Security Act 2015
- Keeping Children Safe in Education 2016
- Working Together to Safeguard Children 2015
- Safeguarding Children and Safer Recruitment in Education 2007
- Local Safeguarding Children Board Guidance
- Guidance for Safer Working Practices 2015
- The Prevent duty – Advice for schools and childcare providers 2015
- What to do if you're worried a child is being abused 2015
- Sexting in schools and colleges: Responding to incidents and safeguarding young people 2016

The Bath and North East Somerset Online Safety Strategy and Wellsway School recommend the use of the Becta PIES model which offers an effective strategic framework for approaching online safety. This model illustrates how a combination of effective policies and practices, education and training, infrastructure and technology underpinned by standards and inspection can be an effective approach to manage and limit online safety risks.




**Becta 2008 – Safeguarding Children in a Digital World**

## 2.2 Online Safety Monitoring

This self-audit has been completed by the member of the School Leadership Team (SLT) responsible for Online Safety. The title for this role is Online Safety Coordinator (OSC). Staff that have contributed to the audit include: Designated Safeguarding Lead, Director of Inclusion, SLT, ICT (Curriculum Lead – Online Safety), Assistant Team Leader ICT, Director of IT Wellsway Multi Academy Trust (WMAT), Assistant Director of IT (WMAT) and the Principal.

| Issue | Action | Notes |
|---|---|---|
| Has the school an online safety policy that complies with available guidance? | Yes | |
| Date of latest update | March 207 | |
| The WSOSP was adopted by governors on | 9.12.09 | And last revised by the Full Governing Body in March 2017 |
| The policy is available for staff at www.wellswayschool.com | Yes | |
| The policy is available for parents/carers at www.wellswayschool.com | Yes | |
| The responsible member of the School Leadership Team is | Mr P Comber | |
| The governor responsible for Online Safety is | Mrs J Ware | |
| The Designated Safeguarding Lead (DSL) is | Mr P Comber | |
| The Online Safety Coordinator (OSC) is | Mr P Comber | |
| The Prevent Single Point of Contact (PSOC) is | Mr P Comber | |
| Is there a clear procedure for a response to an incident of concern? | Yes | See Appendix A |
| Have online safety materials from CEOP and SWGfL been obtained? | Yes | On school website |
| Staff are made aware of the school's Acceptable Use Policy. | Yes | Wellsway School Staff Acceptable Use Policy – Appendix F |
| Students are made aware of the school's Acceptable Use Policy. | Yes | Wellsway School Student Acceptable Use Policy – Appendix G |
| Are all students aware of the school's online safety and receive education on online safety | Yes | e.g. IT Education, assemblies and PSHE |
| Do students know how to report concerns that they might have? | Yes | In Student Planner |
| Do parents/carers sign and return an agreement that their child will comply with the school online safety rules? | Yes | In Student Planner |
| Are staff, students, parents/carers and visitors aware that network and internet use is closely monitored and individual usage can be traced? | Yes | Mentioned in welcome sheet given to visitors. |

| | | |
|---|---|---|
| Personal data is collected, stored and used according to the principles of the Data Protection Act? | Yes | |
| Internet access is provided by an approved educational Internet service provider which complies with DfE requirements. | Yes | SWGfL |
| School-level filtering has been designed to reflect educational objectives and approved by the SLT? | Yes | |
| Staff with responsibility for managing, filtering, network access and monitoring are adequately supervised by a member of SLT? | Yes | Mr D Cooper |
| Appropriate teaching and/or technical members of staff have attended training on the SWGfL filtering system? | Yes | Mr R May |
| Are staff made aware of online safety issues and know how to deal with them? | Yes | Through this and other policies and training |
| Do staff know how to conduct themselves professionally online? | Yes | Through this policy and our Staff Code of Conduct and Wellsway School Online Safety Policy. |
| Are parents/carers given the opportunity to be educated to keep their children safe online? | Yes | Through a variety of sources such as CEOP and B&NES. |
| The Governing Body will receive a report on the implementation of the online policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals. | Yes | FGB annually as part of Child Protection Report. |
| The WSOSP will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be: | | March 2018 |

## 2.3 Key responsibilities for the community

***The key responsibilities of the Wellsway School Senior Leadership Team (SLT) are:***

- Developing, owning and promoting the online safety vision and culture to all stakeholders, in line with national and local recommendations with appropriate support and consultation throughout the school community.
- Ensuring that online safety is viewed by the whole community as a safeguarding issue.
- Supporting the DSL by ensuring they have sufficient time and resources to fulfil their online safety role and responsibilities.
- Ensuring there are appropriate and up-to-date policies and procedures regarding online safety including a Wellsway School Acceptable Use Policy (WSAUP) which covers appropriate professional conduct and use of technology.

- To ensure that suitable and appropriate filtering and monitoring systems are in place to protect students from inappropriate content which meet the needs of the school community whilst ensuring students have access to required educational material.
- To work with and support technical staff in monitoring the safety and security of school systems and networks and to ensure that the school network system is actively monitored.
- Ensuring all members of staff receive regular, up-to-date and appropriate training regarding online safety roles and responsibilities and provide guidance regarding safe appropriate communications.
- Ensuring that online safety is embedded within a progressive whole school curriculum which enables all students to develop an age-appropriate understanding of online safety and the associated risks and safe behaviours.
- To be aware of any online safety incidents and ensure that external agencies and support are liaised with as appropriate.
- Receiving and regularly reviewing online safeguarding records and using them to inform and shape future practice.
- Ensuring there are robust reporting channels for the school community to access regarding online safety concerns, including internal, local and national support.
- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology, including ensuring the safe and responsible use of devices.
- To ensure a member of the Local Governing Body (LGB) is identified with a lead responsibility for supporting online safety.
- Auditing and evaluating current online safety practice to identify strengths and areas for improvement.

***The key responsibilities of the DSL (SLT i/c Online Safety) are:***

- Acting as a named point of contact on all online safeguarding issues and liaising with other members of staff and other agencies as appropriate.
- Ensuring that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- Liaising with the local authority and other local and national bodies, as appropriate.
- Keeping up-to-date with current research, legislation and trends regarding online safety.
- Maintaining a record of online safety concerns/incidents and actions taken as part of the schools safeguarding recording structures and mechanisms.
- To report to the Wellsway School SLT, Local Governing Body and other agencies as appropriate, on online safety concerns and local data/figures.
- Meet regularly with the governor with a lead responsibility for online safety.
- Working with the Wellsway School SLT to review and update the WSOSP, WSAUP and other related policies on a regular basis (at least annually) with stakeholder input.
- Work with the school lead for data protection and data security to ensure that practice is in line with current legislation.
- Coordinating participation in local and national events to promote positive online behaviour, e.g. Safer Internet Day.
- Ensuring that online safety is promoted to parents and carers and the wider community through a variety of channels and approaches.
- Ensuring training and advice for staff is in place.
- Monitor the school online safety incidents to identify gaps/trends and use this data to update the school's education response to reflect need.

- Ensuring an online safety group is in place which includes input from all stakeholder groups.

***The key responsibilities for all members of staff are:***

- Contributing to the development of online safety policies.
- Reading the WSAUP and Wellsway MAT Staff Code of Conduct and adhering to them.
- Taking responsibility for the security of school systems and data.
- Having an awareness of a range of different online safety issues and how they may relate to the children in their care.
- Modelling good practice when using new and emerging technologies.
- Embedding online safety education in curriculum delivery wherever possible.
- Ensuring students understand and follow the WSOSP and WSAUP.
- Developing students understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Monitoring ICT activity in lessons, extra-curricular and extended school activities.
- Reporting any individuals of concern, suspected misuse or problem to the DSL for investigation.
- Being able to signpost to appropriate support available for online safety issues, internally and externally.
- Maintaining a professional level of conduct in their personal use of technology, both on and off site.
- Demonstrating an emphasis on positive learning opportunities.
- Taking personal responsibility for professional development in this area.

***In addition to the above, the key responsibilities for staff managing the technical environment are:***

- Providing a safe and secure technical infrastructure which support safe online practices while ensuring that learning opportunities are still maximised.
- Taking responsibility for the implementation of safe security of systems and data in partnership with the SLT.
- To ensure that suitable access controls and encryption is implemented to protect personal and sensitive information held on school-owned devices.
- Ensuring that the school's filtering policy is applied and updated on a regular basis and that responsibility for its implementation is shared with the line manager and DSL.
- Ensuring that the use of the school's network is regularly monitored and reporting any deliberate or accidental misuse to the line manager and DSL.
- Developing an understanding of the relevant legislation as it relates to the security and safety of the technical infrastructure.
- In conjunction with the line manager and DSL report any breaches and liaising with the local authority (or other local or national bodies) as appropriate on technical infrastructure issues.
- Providing technical support and perspective to the DSL and SLT, especially in the development and implementation of appropriate online safety policies and procedures.
- Ensuring that the school's ICT infrastructure/system is secure and not open to misuse or malicious attack.
- Ensuring that appropriate anti-virus software and system updates are installed and maintained on all setting machines and portable devices.
- Ensure that appropriately strong passwords are applied and enforced for all but the youngest users.
- Ensure SWGfL is informed of issues relating to the filtering applied by the Grid.

***The key responsibilities of children and young people are:***

- Contributing to the development of online safety policies.
- Reading the WSAUP and adhering to it.
- Respecting the feelings and rights of others both on and offline.
- Seeking help from a trusted adult if things go wrong, and supporting others that may be experiencing online safety issues.
- Having a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Needing to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Knowing and understanding 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 WSOSP covers their actions out of school, if related to their membership of the school.

At a level that is appropriate to their individual age, ability and vulnerabilities:

- Taking responsibility for keeping themselves and others safe online.
- Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
- Assessing the personal risks of using any particular technology, and behaving safely and responsibly to limit those risks.

***The key responsibilities of parents and carers are:***

- Reading and signing the WSAUP, encouraging their children to adhere to them, and adhering to them themselves where appropriate.
- Discussing online safety issues with their children, supporting the school in their online safety approaches, and reinforcing appropriate safe online behaviours at home.
- Role modelling safe and appropriate uses of technology and social media.
- Identifying changes in behaviour that could indicate that their child is at risk of harm online.
- Seeking help and support from the school, or other appropriate agencies, if they or their child encounters online problems or concerns.
- Contributing to the development of the school's online safety policies.
- Using school systems safely and appropriately.
- Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.

***Community Users***

- Community Users who access school IT systems as part of the Extended School provision will be expected to sign the WSAUP before being provided with access to school systems.

## 2.4 Authorising internet access

- The school will maintain a current record of all staff and students who are granted access to the school's devices and systems.
- All staff, students and visitors will read and sign the WSAUP before using any school resources.
- Parents will be informed that students will be provided with supervised Internet access which is appropriate to their age and ability.
- Parents will be asked to read the WSAUP for student access and discuss it with their child, where appropriate.
- Parents or carers of all students are given the opportunity to opt out of internet access.
- When considering access for vulnerable members of the community (such as with students with special education needs) the school will make decisions based on the specific needs and understanding of the student(s).
- Student or staff access to the internet can be withdrawn should it be deemed necessary by the relevant member of SLT.

## 2.5 Responding to Online Incidents and Safeguarding Concerns (Summary - Appendix A)

- All members of the community will be made aware of the range of online risks that are likely to be encountered including sexting, online/cyber bullying etc. This will be highlighted within staff training and educational approaches for students.
- All members of the school/setting community will be informed about the procedure for reporting online safety (e-Safety) concerns, such as breaches of filtering, sexting, cyberbullying, illegal content etc.
- The DSL will be informed of any online safety (e-Safety) incidents involving child protection concerns, which will then be recorded.
- The DSL will ensure that online safety concerns are escalated and reported to relevant agencies in line with the B&NES Safeguarding Children Board thresholds and procedures.
- Complaints about internet misuse will be dealt with under the School's complaints procedure.
- Complaints about online/cyber bullying will be dealt with under the School's anti-bullying policy and procedure
- Any complaint about staff misuse will be referred to the Principal.
- Any allegations against a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer).
- Students, parents and staff will be informed of the schools complaints procedure.
- Staff will be informed of the complaints and whistleblowing procedure.
- All members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns.
- All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community.
- The school will manage online safety (e-Safety) incidents in accordance with the Wellsway School Behaviour for Learning Policy where appropriate.
- The school will inform parents/carers of any incidents of concerns as and when required.
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes as required.
- Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact the Police via 101 or 999 if there is immediate danger or risk of harm.

- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to Kent Police.
- If the school is unsure how to proceed with any incidents of concern, then the incident will be escalated to the Education Safeguarding Team.
- Parents and children will need to work in partnership with the school to resolve issues.

## 2.6 Online Communication and Safer Use of Technology

***Managing the school website***

- The school will ensure that information posted on the school website meets the requirements as identified by the Department for Education (DfE).
- The contact details on the website will be the school address, email and telephone number. Staff or students' personal information will not be published.
- The Principal will take overall editorial responsibility for online content published and will ensure that information is accurate and appropriate.
- The website will comply with the school's guidelines for publications including accessibility respect for intellectual property rights, privacy policies and copyright.
- Parents or carers can state that their child's work should not be published on the school website or other online space. Parents are reminded of this annually via the school newsletter.
- The administrator account for the school website will be safeguarded with an appropriately strong password.
- The school will post information about safeguarding, including online safety, on the school website for members of the community.

***Publishing images and videos online***

- No student will be identified in an image/video by their full names on the school website or other public online space without parental or carer consent.
- Parents or carers can state that no image/video focusing on their child is to be published on the school website or other online space. Parents are reminded of this annually via the school newsletter.

***Managing email***

- Students may only use school provided email accounts for educational purposes.
- All members of staff are provided with a specific school email address to use for any official communication.
- The use of personal email addresses by staff for any official school business is not permitted.
- The forwarding of any chain messages/emails etc. is not permitted. Spam or junk mail will be blocked and reported to the email provider.
- Any electronic communication which contains any content which could be subject to data protection legislation (e.g. sensitive or personal information) will only be sent in an attachment which is password protected..
- Access to school email systems will always take place in accordance to data protection legislation and in line with other appropriate school policies e.g. confidentiality.
- Members of the community must immediately tell the OSC if they receive offensive communication and this will be recorded in the school safeguarding files/records.

- Staff will be encouraged to develop an appropriate work life balance when responding to email, especially if communication is taking place between staff and students and parents.
- Excessive social email use can interfere with teaching and learning and will be restricted. Access in school to external personal email accounts may be blocked.
- Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper would be.
- School email addresses and other official contact details will not be used for setting up personal social media accounts.

***Official videoconferencing and webcam use for educational purposes***

- The school acknowledges that videoconferencing is a challenging activity with a wide range of learning benefits. Preparation and evaluation are essential to the whole activity.
- All videoconferencing equipment will be switched off when not in use and where appropriate, not set to auto answer.
- Equipment connected to the educational broadband network will use the national E.164 numbering system and display their H.323 ID name.
- External IP addresses will not be made available to other sites.
- Videoconferencing contact details will not be posted publically.
- Video conferencing equipment will be kept securely and, if necessary, locked away when not in use.
- School videoconferencing equipment will not be taken off school premises without permission.
- Staff will ensure that external videoconference opportunities and/or tools are suitably risk assessed and will ensure that accounts and systems used to access events are appropriately safe and secure.

***Users***

- Students will ask permission from a teacher before making or answering a videoconference call or message.
- Videoconferencing will be supervised appropriately for the students' age and ability.
- Parents and carers consent will be obtained prior to students taking part in videoconferencing activities.
- Video conferencing will take place via official and approved communication channels following a robust risk assessment.
- Only key administrators will be given access to videoconferencing administration areas or remote control pages.
- Unique log on and password details for the educational videoconferencing services will only be issued to members of staff and kept secure.

***Content***

- When recording a videoconference lesson, written permission will be given by all sites and participants. The reason for the recording must be given and the recording of videoconference should be clear to all parties at the start of the conference. Recorded material will be stored securely.
- If third party materials are to be included, the school will check that recording is acceptable to avoid infringing the third party intellectual property rights.

- The school will establish dialogue with other conference participants before taking part in a videoconference. If it is a non-school site the school will check that they are delivering material that is appropriate for the class.

***Managing personal data online***

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

Wellsway School will ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".
- It has a Data Protection Policy (Appendix E)
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
- Risk assessments are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from information risk incidents
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties
- There are clear policies about the use of cloud storage / cloud computing which ensure that such data transfer / storage meets the requirements laid down by the Information Commissioner's Office.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices wherever possible, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Take care to ensure that personal data is not displayed in a public space e.g. via a data projector in a classroom.
- Password protect files which contain sensitive information and are attached to emails.

When personal data is stored on any portable computer system, USB stick or any other removable media:

- Whenever possible ensure the opportunity is taken use password protected media and programs.
- The data must be securely deleted from the device once it has been transferred or its use is complete.
- Staff should take care to ensure that data, whether in paper or electronic format, is stored safely and discreetly at home and when in transit outside of school. Every reasonable measure should be taken to keep data private.

# 3.0 Education and Training

## 3.1 Teaching and learning

***Appropriate and safe classroom use of the internet and any associated devices***

- Internet use is a key feature of educational access and all students will receive age and ability appropriate education to support and enable them to develop strategies to respond to concerns as part of an embedded whole school curriculum. Please access specific curriculum policies for further information.
- The school's internet access will be designed to enhance and extend education.
- All members of staff are aware that they cannot rely on filtering alone to safeguard students and supervision, classroom management and education about safe and responsible use is essential.
- Supervision of students will be appropriate to their ability and understanding.
- All school owned devices will be used in accordance with the WSAUP and with appropriate safety and security measure in place.
- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.
- Students will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.
- The school will use age appropriate search tools as decided by the school following an informed risk assessment to identify which tool best suits the needs of our community.
- The school will ensure that the use of internet-derived materials by staff and students complies with copyright law and acknowledge the source of information.
- The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.
- The school will use the internet to enable students and staff to communicate and collaborate in a safe and secure environment.

## 3.2 Online Safety for students with special educational needs

A student who has a learning difficulty or disability may be even more vulnerable to deceptive messages offering friendship or to opening dialogue on topics of mutual interest. For example, many students with autistic spectrum disorder take messages very literally and could be persuaded to act upon them. These students are likely to need additional advice on safe behaviours and what they should never disclose to

others online; they may also need increased supervision. This could include, for example, guidance that before entering dialogue with anyone new, they should always consult a trusted adult.

## 3.3 Engagement Approaches

***Engagement and education of children and young people***

- An online safety curriculum will be established and embedded throughout the whole school, to raise awareness regarding the importance of safe and responsible internet use amongst students.
- Education about safe and responsible use will precede internet access.
- Students input will be sought when writing and developing school online safety policies and practices, including curriculum development and implementation.
- Students will be supported in reading and understanding the WSAUP in a way which suits their age and ability.
- All users will be informed that network and internet use will be monitored.
- Online safety will be included in the PSHE, SRE and ICT programmes of study, covering both safe school and home use.
- Online safety education and training will be included as part of the transition programme across the Key Stages and when moving between establishments.
- Acceptable Use expectations and posters will be posted in all rooms with internet access.
- Safe and responsible use of the internet and technology will be reinforced across the curriculum and within all subject areas.
- External support will be used to complement and support the schools internal online safety education approaches.
- The school will reward positive use of technology by students.
- The school will implement peer education to develop online safety as appropriate to the needs of the students.

***Engagement and education of staff***

- The Online Safety (e-Safety) Policy will be formally provided to and discussed with all members of staff as part of induction and will be reinforced and highlighted as part of our safeguarding responsibilities.
- Staff will be made aware that our internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential when using school systems and devices.
- Up-to-date and appropriate staff training in safe and responsible internet use, both professionally and personally, will be provided for all members of staff in a variety of ways, on a regular (at least annual) basis.
- All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

***Engagement and education of parents and carers***

- Wellsway School recognises that parents/carers have an essential role to play in enabling children to become safe and responsible users of the internet and digital technology.

- Parents' attention will be drawn to the school online safety (e-Safety) policy and expectations in newsletters, letters, school prospectus and on the school website.
- A partnership approach to online safety at home and at school with parents will be encouraged. This may include offering parent evenings with demonstrations and suggestions for safe home internet use or highlighting online safety at other well attended events e.g. parent evenings, transition events, fetes and sports days.
- Parents will be requested to read online safety information as part of the Home School Agreement.
- Parents will be encouraged to read the WSAUP for students and discuss its implications with their children.
- Information and guidance for parents on online safety will be made available to parents in a variety of formats.
- Parents will be encouraged to role model positive behaviour for their children online.

# 4.0 Infrastructure and Technology

***Managing Information Systems***

## 4.1 Security and Management of Information Systems

- Wellsway School will be responsible for ensuring that the school network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. A more detailed Technical Security Policy can be found in Appendix D.
- The security of the school information systems and users will be reviewed regularly.
- Virus protection will be updated regularly.
- Personal data sent over the internet or taken off site (such as via portable media storage) will be encrypted or accessed via appropriate secure remote access systems.
- Portable media may not be used without specific permission followed by an anti-virus /malware scan.
- Unapproved software will not be allowed in work areas or attached to email.
- Files held on the school's network will be regularly checked.
- The computing coordinator/network manager will review system capacity regularly.
- The appropriate use of user logins and passwords to access the school network will be enforced for all but the youngest users.
- All users will be expected to log off or lock their screens/devices if systems are unattended.
- The school will log and record internet use on all school owned devices.

## 4.2 Password policy

- All users will be informed not to share passwords or information with others and not to login as another user at any time.
- Staff and students must always keep their password private and must not share it with others or leave it where others can find it.
- All members of staff will have their own unique username and private passwords to access school systems. Members of staff are responsible for keeping their password private.

- All students are provided with their own unique username and private passwords to access school systems. Students are responsible for keeping their password private.
- We require staff and students to use STRONG passwords for access into our system.
- We require staff and students to change their passwords every two years.

## 4.3 Filtering and Monitoring

- The governors/proprietors will ensure that the school has age and ability appropriate filtering and monitoring in place whilst using school devices and systems to limit student's exposure to online risks.
- The school's internet access strategy will be dependent on the need and requirements of our community and will therefore be designed to suit the age and curriculum requirements of our students, with advice from technical, educational and safeguarding staff.
- All monitoring of school owned/provided systems will take place to safeguard members of the community.
- All users will be informed that use of school systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.
- The school uses educational filtered secure broadband connectivity through the KPSN which is appropriate to the age and requirement of our students.
- The school uses Light Speed filtering system which blocks sites that fall into categories such as pornography, racial hatred, extremism, gaming, sites of an illegal nature, etc.
- The school will ensure that filtering policy is continually reviewed.
- The school will have a clear procedure for reporting breaches of filtering which all members of the school community (all staff and all students) will be made aware of.
- If staff or students discover unsuitable sites, the URL will be reported to the DSL and will then be recorded and escalated as appropriate.
- The School will use a web content filtering product which will as a minimum:
    - Subscribe to the Internet Watch Foundation Child Abuse Images and Content (CAIC) URL List;
    - Block 100% of illegal material identified by the Internet Watch Foundation (IWF);
    - Capable of blocking 90% of inappropriate content in each of the following categories:
        - Pornographic, adult, tasteless or offensive material;
        - Violence (including weapons and bombs);
        - Racist, extremist and hate material;
        - Illegal drug taking and promotion;
- Criminal skills and software piracy.
- Changes to the school filtering policy will be risk assessed by staff with educational and technical experience prior to any changes and where appropriate with consent from the Leadership Team.
- All changes to the school filtering policy will be logged and recorded.
- The SLT will ensure that regular checks are made to ensure that the filtering methods selected are effective and appropriate.
- Any material that the school believes is illegal will be reported to appropriate agencies.

## 4.4 Management of applications (apps) used to record children's progress

- The Principal is ultimately responsible for the security of any data or images held of children.
- Apps/systems which store personal data will be risk assessed prior to use.

- Only school/setting issued devices will be used for apps that record and store children's personal details, attainment or photographs. Personal staff mobile phones or devices will not be used to access or upload content to any apps which record and store children's personal details, attainment or images.
- Devices will be appropriately encrypted if taken off site to prevent a data security breach in the event of loss or theft.
- Users will be advised on safety measures to protect all members of the community such as using strong passwords, logging out of systems etc.
- Parents will be informed of the schools expectations regarding safe and appropriate use (e.g. not sharing passwords or sharing images) prior to being given access.

# 5.0 Social Media Policy

## 5.1 General social media use

- Expectations regarding safe and responsible use of social media will apply to all members of Wellsway School community and exist in order to safeguard both the school and the wider community, on and offline. Examples of social media may include blogs, wikis, social networking sites, forums, bulletin boards, multiplayer online gaming, apps, video/photo sharing sites, chatrooms, instant messenger and many others.
- All members of Wellsway School community will be encouraged to engage in social media in a positive, safe and responsible manner at all times.
- Information about safe and responsible use of social media will be communicated clearly and regularly to all members of Wellsway School community.
- All members of Wellsway School's community are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.
- The school will control student and staff access to social media and social networking sites whilst on site and when using school provided devices and systems.
- The use of social networking applications during school hours for personal use **is not** permitted by staff and students.
- Any concerns regarding the online conduct of any member of Wellsway School community on social media sites should be reported to the OSC or Principal (staff concerns) and will be managed in accordance with policies such as anti-bullying, code of conduct, allegations against staff, behaviour and safeguarding/child protection.
- Any breaches of school policy may result in criminal, disciplinary or civil action being taken and this will depend upon the age of those involved and the circumstances of the wrong committed. Action taken will be accordance with relevant policies, such as anti-bullying, code of conduct, allegations against staff, behaviour and safeguarding/child protection.

## 5.2 Official use of social media

- *Wellsway School has established* official social media channels.

- Official use of social media sites by the school will only take place with clear educational or community engagement objectives with specific intended outcomes e.g. increasing parental engagement.
- Official use of social media sites as communication tools will be risk assessed and formally approved by the Principal.
- Staff will use school provided email addresses to register for and manage any official approved social media channels.
- Members of staff running official social media channels will sign a specific WSAUP to ensure they are aware of the required behaviours and expectations of use and to ensure that sites are used safely, responsibly and in accordance with local and national guidance and legislation.
- All communication on official social media platforms will be clear, transparent and open to scrutiny.
- Any online publication on official social media sites will comply with legal requirements including the Data Protection Act 1998, right to privacy conferred by the Human Rights Act 1998, or similar duty to protect private information and will not breach any common law duty of confidentiality, copyright etc.
- Official social media use will be in line with existing policies including anti-bullying and child protection.
- Images or videos of children will only be shared on official social media sites in accordance with the advice in this policy.
- Information about safe and responsible use of social media channels will be communicated clearly and regularly to all members of the community.
- Official social media sites, blogs or wikis will be suitably protected (e.g. password protected) and where possible/appropriate, run and/or linked to from the school website and take place with written approval from the SLT.
- Leadership staff must be aware of account information and relevant details for social media channels in case of emergency, such as staff absence.
- Public communications on behalf of the school will, where possible, be read and agreed by at least one other colleague.
- Official social media channels will link back to the school website and/or WSAUP to demonstrate that the account is official.
- The school will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels.

## 5.3 Staff personal use of social media

- The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.
- Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of the WSAUP.
- All members of staff are advised not to communicate with or add as ‘friends’ any current or past students or current or past students’ family members via any personal social media sites, applications or profiles. Any pre-existing relationships or exceptions that may compromise this will be discussed with Designated Safeguarding Lead and/or the Principal.
- Staff will discuss the circumstances with the Principal if ongoing contact with students is required once they have left the school roll,
- All communication between staff and members of the school community on school business will take place via official approved communication channels.

- Any communication from students/parents received on personal social media accounts will be reported to the schools designated safeguarding lead.
- Information and content that staff members have access to as part of their employment, including photos and personal information about students and their family members, colleagues etc. will not be shared or discussed on personal social media sites.
- All members of staff are strongly advised to safeguard themselves and their privacy when using social media sites. This will include being aware of location sharing services, setting the privacy levels of their personal sites as strictly as they can, opting out of public listings on social networking sites, logging out of accounts after use and keeping passwords safe and confidential.
- All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional role and is in accordance with schools policies and the wider professional and legal framework.
- Members of staff will notify the OSC immediately if they consider that any content shared or posted via any information and communications technology, including emails or social networking sites conflicts with their role in the school/setting.
- Members of staff are encouraged not to identify themselves as employees of Wellsway School on their personal social networking accounts. This is to prevent information on these sites from being linked with the school and also to safeguard the privacy of staff members and the wider community.
- Members of staff will ensure that they do not represent their personal views as that of the school on social media.
- School email addresses will not be used for setting up personal social media accounts.
- Members of staff who follow/like the school's social media channels will be advised to use dedicated professionals accounts, where possible, to avoid blurring professional boundaries.

## 5.4 Staff official use of social media

- If members of staff are participating in online activity as part of their capacity as an employee of the school, then they are requested to be professional at all times and to be aware that they are an ambassador for the school.
- Staff using social media officially will always act within the legal frameworks they would adhere to within the workplace, including libel, defamation, confidentiality, copyright, data protection as well as equalities laws.
- Staff must ensure that any image posted on any official social media channel complies with the school's policies in relation to written parental consent.
- Staff using social media officially will be accountable and must not disclose information, make commitments or engage in activities on behalf of the school unless they are authorised to do so.
- Staff using social media officially will inform their line manager, the Designated Safeguarding Lead and/or the Principal of any concerns such as criticism or inappropriate content posted online.
- Staff will not engage with any direct or private messaging with students or parents/carers through social media and will communicate via official communication channels.
- Staff using social media officially will sign the WSAUP.

### *5.5 Students use of social media*

- Safe and responsible use of social media sites will be outlined for students and their parents as part of the WSAUP.

- Personal publishing on social media sites will be taught to students as part of an embedded and progressive education approach via age appropriate sites which have been risk assessed and approved as suitable for educational purposes.
- Students will be advised to consider the risks of sharing personal details of any kind on social media sites which may identify them and / or their location. Examples would include real/full name, address, mobile or landline phone numbers, school attended, Instant messenger contact details, email addresses, full names of friends/family, specific interests and clubs etc.
- Students will be advised not to meet any online friends without a parent/carer or other responsible adult's permission and only when they can be present.
- Students will be advised on appropriate security on social media sites and will be encouraged to use safe and passwords, deny access to unknown individuals and be supported in learning how to block and report unwanted communications.
- Students will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private/protected.
- Any official social media activity involving students will be moderated by the school where possible.
- The school is aware that many popular social media sites state that they are not for students under the age of 13, therefore the School will not create accounts within school specifically for children under this age.
- Any concerns regarding students' use of social networking, social media and personal publishing sites, both at home and at school, will be dealt with in accordance with existing school policies including anti-bullying and behaviour.
- Any concerns regarding students' use of social networking, social media and personal publishing sites, both at home and at school, will be raised with parents/carers, particularly when concerning any underage use of social media sites.

# 6.0 Use of Personal Devices and Mobile Phones

## 6.1 Rationale regarding personal devices and mobile phones

- The widespread ownership of mobile phones and a range of other personal devices among students and adults will require all members of Wellsway School community to take steps to ensure that mobile phones and personal devices are used responsibly within and outside of school.
- The use of mobile phones and other personal devices by students and adults will be decided by the school and is covered in appropriate policies including the Mobile Phone Policy.

## 6.2 Expectations for safe use of personal devices and mobile phones

- All use of personal devices and mobile phones will take place in accordance with the law and other appropriate school policies
- Electronic devices of all kinds that are brought in on site are the responsibility of the user at all times. The school accepts no responsibility for the loss, theft or damage of such items. Nor will the school accept responsibility for any adverse health effects caused by any such devices either potential or actual.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the community and any breaches will be dealt with as part of the behaviour for learning policy and anti-bullying policy.

- Members of staff will be issued with a work phone number and email address where contact with students or parents/carers is required.
- All members of Wellsway School community will be advised to take steps to protect their mobile phones or devices from loss, theft or damage.
- All members of Wellsway School community will be advised to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices if they are lost or stolen. Passwords and pin numbers should be kept confidential. Mobile phones and personal devices should not be shared.
- All members of Wellsway School community will be advised to ensure that their mobile phones and personal devices do not contain any content which may be considered to be offensive, derogatory or would otherwise contravene the school policies.
- School mobile phones and devices must always be used in accordance with the WSAUP.
- School mobile phones and devices used for communication with parents and students must be suitably protected via a passcode/password/pin and must only be accessed and used by members of staff.

## 6.3 Students use of personal devices and mobile phones

- Students will be educated regarding the safe and appropriate use of personal devices and mobile phones.
- All use of mobile phones and personal devices by students will take place in accordance with the Mobile Phone and Electronic Device Policy.
- Student's personal mobile phones and personal devices will be kept in a secure place, switched off and kept out of sight during school hours.
- If a student needs to contact his/her parents/carers they will be allowed to use a school phone outside of lesson time.
- Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.
- Students should protect their phone numbers by only giving them to trusted friends and family members.
- Students will be instructed in safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences.
- Mobile phones and personal devices must not be taken into examinations. Students found in possession of a mobile phone or personal device during an exam will be reported to the appropriate examining body. This may result in the student's withdrawal from either that examination or all examinations.
- School staff may confiscate a student's mobile phone or device if they believe it is being used to contravene the schools behaviour or bullying policy or could contain youth produced sexual imagery (sexting). The phone or device may be searched by a member of the SLT. Searches of mobile phone or personal devices will only be carried out in accordance with the DfE guidance which can be found at the following link: https://www.gov.uk/government/publications/searching-screening-and-confiscation
- If there is suspicion that material on a student's personal device or mobile phone may be illegal or may provide evidence relating to a criminal offence then the device will be handed over to the police for further investigation.

## 6.4 Staff use of personal devices and mobile phones

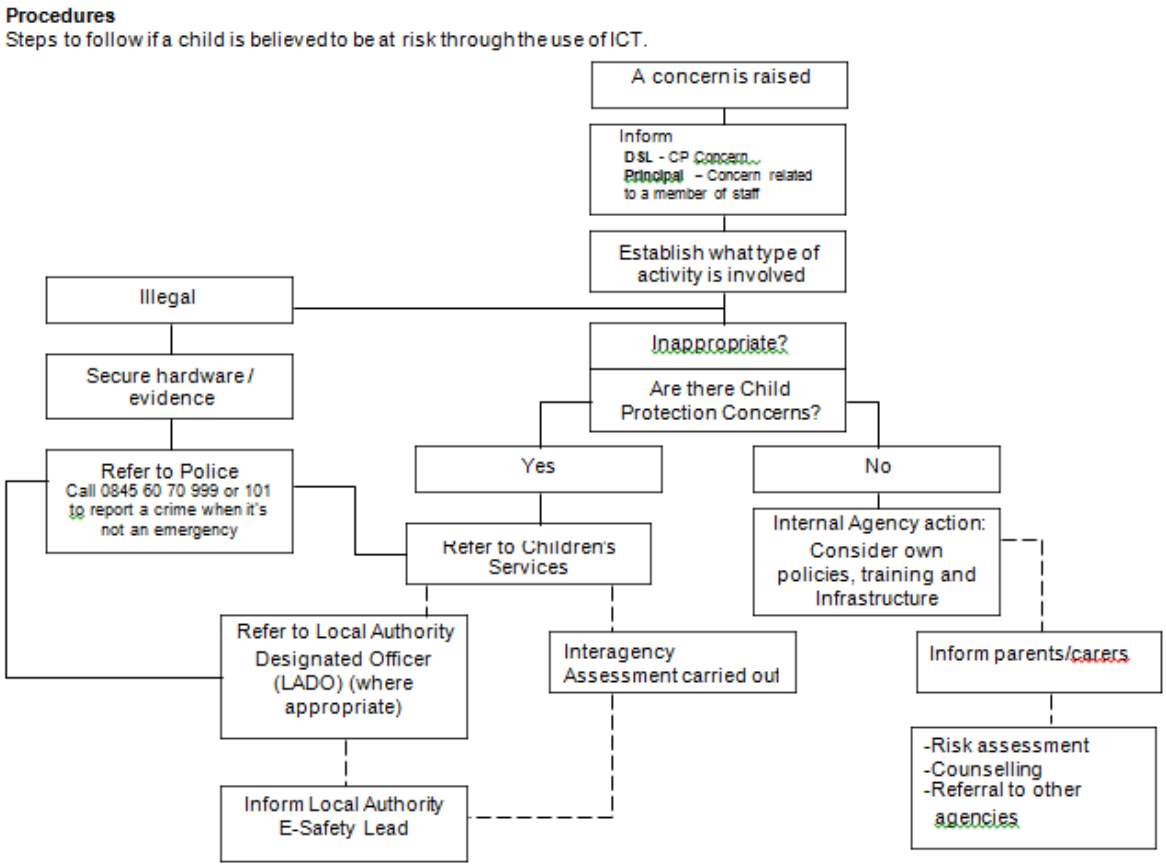
- Members of staff are not permitted to use their own personal phones or devices for contacting students and their families within or outside of the setting in a professional capacity. Any pre-existing relationships which could compromise this will be discussed with their line manager.
- Staff will not use personal devices such as mobile phones, tablets or cameras to take photos or videos of children and will only use work-provided equipment for this purpose.
- Staff personal mobile phones and devices will be switched off/switched to 'silent' mode during lesson times.
- Bluetooth or other forms of communication should be "hidden" or switched off during lesson times.
- Personal mobile phones or devices will not be used during teaching periods unless permission has been given by a member of the Leadership Team in emergency circumstances.
- Staff will ensure that any content bought on site via mobile phones and personal devices are compatible with their professional role and expectations.
- If a member of staff breaches the school policy then disciplinary action will be taken.
- If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence then the police will be contacted.
- Any allegations against members of staff involving personal use of mobile phone or devices will be responded to following the allegations management policy.

## 6.5 Visitors use of personal devices and mobile phones

- Parents/carers and visitors must use mobile phones and personal devices in accordance with the school's acceptable use policy.
- Use of mobile phones or personal devices by visitors and parents/carers to take photos or videos is not allowed by parents/carers on school site.
- The school will ensure appropriate signage and information is displayed and provided to inform visitors of expectations of use.
- Staff will be expected to challenge concerns when safe and appropriate and will always inform the DSL of any breaches of use by visitors.

# Appendix A:

**Guidance from B&NES Local Authority on what to do if a concern is raised following an online safety incident:**



# Appendix B:

**Responding to concerns regarding radicalisation and extremism online**

- The school will take all reasonable precautions to ensure that children are safe from terrorist and extremist material when accessing the internet in schools and that suitable filtering is in place which takes into account the needs of students.
- When concerns are noted by staff that a child may be at risk of radicalisation online then the Designated Safeguarding Lead (DSL) will be informed immediately and action will be taken in line with the safeguarding policy.
- Online hate content directed towards or posted by specific members of the community will be responded to in line with existing school policies, including anti-bullying, behaviour etc. If the school is unclear if a criminal offence has been committed then the Designated Safeguarding Lead will obtain advice immediately via the B&NES Safeguarding Team and/or Avon and Somerset Police.

# Appendix C

### Information & Organisations

| |
|---|
| **CEOP** - The Child Exploitation and Online Protection Centre is part of UK police and is dedicated to protecting children from sexual abuse wherever they may be. That means building intelligence around the risks, tracking and bringing offenders to account either directly or with local and international forces and working with children and parents to deliver our unique Think U Know educational programme.<br>http://ceop.police.uk |
| **Childnet International's** mission is to work in partnership with others around the world to help make the Internet a great and safe place for children.<br>Childnet works in 3 main areas of Access, Awareness, Protection & Policy.<br>http://www.childnet.com |
| **DfE** - The Department for Education is responsible for education and children's services.<br>http://www.education.gov.uk |
| **IWF** – The Internet Watch Foundation was established in 1996 by the UK internet industry to provide the UK internet 'Hotline' for the public and IT professionals to report potentially illegal online content within their remit and to be the 'notice and take-down' body for this content. IWF works in partnership with the online industry, law enforcement, government, the education sector, charities, international partners and the public to minimise the availability of this content, specifically, child sexual abuse content hosted anywhere in the world and criminally obscene and incitement to racial hatred content hosted in the UK.<br>http://www.iwf.org.uk |
| **Know IT All for Parents** contains advice for parents and carers, and a special section for children and young people.<br>http://www.childnet.com/kia/parents/ |
| **Local Safeguarding Children Board**<br>http://www.bathnes.gov.uk/services/children-young-people-and-families/child-protection/local-safeguarding-children-board |
| **Report Abuse**<br>http://ceop.police.uk/safety-centre |

**UK Safer Internet Centre (UKSIC)** - The UK Safer Internet Centre is co-funded by the European Commission and brought to you by a partnership of three leading organisations, Childnet International, the South West Grid for Learning and the Internet Watch Foundation. The UK Safer Internet Centre has three main functions: An Awareness Centre, a Helpline and a Hotline.
http://www.saferinternet.org.uk

# Appendix D – Staff Acceptable Use 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 access to the internet and digital technologies 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 communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for *students* learning and will, in return, expect staff and volunteers to agree to be responsible users.

### Acceptable Use Policy Agreement

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

For my professional and personal safety:

- I understand that the *school* will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, VLE etc.) out of school, and to the transfer of personal data (digital or paper based) out of school.

- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school. (schools should amend this section in the light of their policies which relate to the personal use, by staff and volunteers, of school systems)
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using *school academy* ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (eg on the school website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites in school in accordance with the school's policies.
- I will only communicate with students / pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner

- I will not engage in any on-line 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 / academy*:

- When I use my mobile devices (laptops / tablets / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using *school* equipment. I will also follow any additional rules 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 ICT systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted , or if I have any concerns about the validity of the email (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 / academy policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.

- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school / academy equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Data Policy. Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.
- I understand that data protection policy requires that any staff or student / 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 / academy 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 the *school / academy*:
- I understand that this Acceptable Use Policy applies not only to my work and use of school / academy digital technology equipment in school, but also applies to my use of school / academy systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school / academy
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors / Directors and / or the Local Authority and in the event of illegal activities the involvement of the police.

# Appendix E – Student Acceptable Use Policy

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These 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. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Agreement is intended to ensure:
- that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and will have good access to digital technologies to enhance their learning and will, in return, expect the *students / pupils* to agree to be responsible users.

**Acceptable Use Policy Agreement**

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

For my own personal safety:

- I understand that the *school / academy* will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line (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 / academy* 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 / academy* systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (eg 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 / academy*:

- I will only use my own personal devices (mobile phones / USB devices etc) in school if I have permission. I understand that, if I do use my own devices in the *school / academy*, 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 this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person / organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)

- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.
- I will only use social media sites with permission and at the times that are allowed

When using the internet for research or recreation, I recognise that:

- I should 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 try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the *school / academy* also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include (schools / academies should amend this section to provide relevant sanctions as per their behaviour policies) loss of access to the school network / internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.