E-Safety Policy

Chew Valley School

1.Scope of the Policy

This policy applies to all members of the school community (including staff, students, volunteers, parents/carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school. A glossary of terms is attached at Appendix 1.

2. Policy Statements

2. 1 Education–Students

2.1 .1 Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

2.1.2 The school implements an acceptable use policy for staff (Appendix 2) and students (Appendix 3).

2.2. 3 E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum. The e-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned e-safety curriculum is provided as part of Computing lessons and is regularly revisited.
- Key e-safety messages are reinforced as part of a planned programme of assemblies and tutorial/pastoral activities.
- Students are taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.
- Students are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices.
- In lessons where internet use is pre-planned, it is best practice that students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where students are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

2.2 Education & Training–Staff

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

- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school E-safety Policy and Acceptable Use Agreements.
- All staff will receive annual "refresher" training in e-safety as part of their annual child protection/safeguarding briefing.

2.3 Technical–Infrastructure/Equipment, Filtering & Monitoring

2.2.1 The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. The following applies to infrastructure/equipment, filtering and monitoring.

- All users will be provided with a username and secure password generated by the Network Manager who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password and will be required to change their password every 90 days.
- The "master/administrator" passwords for the school ICT system, used by the Network Manager is also available to the Headteacher and Deputy Headteacher, and is kept securely in the school safe.
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored.
- School technical staff regularly monitor and record the activity of users on the school technical systems including Impero and users are made aware of this in the Acceptable Use Agreement.

2.4 Use of Digital and Video Images

The following principles apply to the use of digital and video images:

- When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.
- In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other students in the digital/video images.
- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital/video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.
- Students'/Pupils' full names should not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of students are published on the school website as part of the Home School Agreement.

2.5 Social Media

2.5.1 See the Social Media Policy (Appendix 4) for more information.

2.5.2 The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to students, staff and the school through limiting access to personal information:

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions.
- Risk assessment, including legal risk.

2.5.3 School staff should ensure that:

- No reference should be made in personal social media to students, parents/carers or school staff.
- They do not engage in online discussion on personal matters relating to members of the school community.
- Personal opinions should not be attributed to the school or local authority.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

2.5.4 The school's use of social media for professional purposes will be checked regularly by the Deputy Headteacher to ensure compliance with the Social Media and Data Protection Policies.

3. Responding to Incidents of Misuse

3.1 Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, the police will be informed.

3.2 Other Incidents

3.2.1 It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

3.2.2 In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below).
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
    - Internal response or discipline procedures.
    - Involvement by Local Authority or national / local organisation (as relevant).
    - Police involvement and/or action.
- If content being reviewed includes images of child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
    - incidents of 'grooming' behaviour.
    - the sending of obscene materials to a child.
    - adult material which potentially breaches the Obscene Publications Act.
    - criminally racist material.
    - other criminal conduct, activity or materials.
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

3.2.3 It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes.

Appendices

Can be found on the following pages:

- **Appendix 4: Glossary of Terms**
- **Appendix 2: School Acceptable Use Policy (AUP)**
- **Appendix 3: Student Acceptable Use Policy**
- **Appendix 4: Social Media Policy**

Policy agreed by governors: November 2014

Policy to be reviewed: November 2015

Appendix 1
Glossary of terms

AUP	Acceptable Use Policy – see templates earlier in this document
CEOP	Child Exploitation and Online Protection Centre (part of UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes
CPC	Child Protection Committee
CPD	Continuous Professional Development
CYPS	Children and Young Peoples Services (in Local Authorities)
FOSI	Family Online Safety Institute
EA	Education Authority
ES	Education Scotland
HWB	Health & Well-being
ICO	Information Commissioners Officer
ICT	Information & Communications Technology
ICTMark	Quality standard for schools provided by NAACE
INSET	In Service Education & Training
IP address	The label that identifies each computer to other computers using the IP (Internet protocol)
ISP	Internet Service Provider
ISPA	Internet Service Providers' Association
IWF	Internet Watch Foundation
LA	Local Authority
LAN	Local Area Network
MIS	Management Information System
NEN	National Education Network – works with the Regional Broadband Consortia (e.g. SWGfL) to provide the safe broadband provision to schools across Britain
Ofcom	Office of Communications (independent communications sector regulator)
SLT	Senior Management Team
SWGfL	South West Grid for Learning Trust – the Regional Broadband Consortium of SW Local Authorities – is the provider of broadband and other services for schools and other organisations in the SW

TUK	Think U Know – educational e-safety programmes for schools, young people and parents
VLE	Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting
WAP	Wireless Application Protocol

Appendix 2

Chew Valley School ICT Acceptable Use Policy (AUP)

A. Purpose

Chew Valley School seeks to promote and facilitate the proper and extensive use of Information Technology in the interests of learning, teaching, research, administration and management. This requires responsible and legal use of the technologies and facilities made available to students, staff and visitors of the school. It has been drawn up to protect all parties - the pupils, the staff and the school. This Acceptable Use Policy is intended to provide a framework for such use of Chew Valley School's IT resources.
Users of these services and facilities, have access to valuable school resources, to sensitive data, and to internal and external networks. Consequently, it is important for users to behave in a responsible, ethical, and legal manner.

B. Scope

This policy applies to all users of computing resources owned or managed by the school. Individuals covered by the policy include (but are not limited to) staff, students, guests of the administration, and external individuals accessing network services via the school's computing facilities.
Computing resources include all school owned, licensed, or leased hardware and software, and use of the school network via a physical or wireless connection, regardless of the ownership of the computer or device connected to the network.

C. Acceptable Use

1. Each network user is given their own work area protected by a username and password. As such, each user has privacy and confidentiality and is therefore expected not to breach security in any way. Each network user is solely responsible for his/her own account and on no occasion is any user to access another user's account.
2. Passwords are an essential aspect of the security of the school's resources and they provide an important first line of protection for the Student Records, School's Shared Documents, School Emails, Electronic Resources and personal Documents that are stored in our system. Having a strong password is one way that each User can contribute to the school's overall security. Strong passwords help the school prevent unauthorised or inappropriate access to various Electronic Resources like email accounts, personal documents, student information systems, financial records, file repositories and administrative/transactional systems.
3. All Users must maintain a password that meets the following minimum requirements:
    - Must be a MINIMUM of 8 characters
    - At least one upper case alphabetic character (A-Z)
    - At least one lower case alphabetic character (a-z)
    - At least one number

- No blank spaces

4. Passwords will automatically expire after 90 days and must be changed. All users will be notified well in advance of their password expiring so that they may reset them without interruption in access to the school's network.
5. All traffic involving the Internet and e-mail is constantly logged and, in the unlikely event of a problem, the school reserves the right to examine and/or delete any files that may be held on the school network computer system.
6. The school is using Microsoft's Office 365 services and all users should agree with the Microsoft Office 365 Acceptable Use Policy (AUP) and Terms of Use (TOU) agreements.
7. Activity that threatens the integrity of any of the school ICT systems is forbidden and the copyright of materials must be respected.
8. All Internet use should be appropriate to staff professional activity or to pupils' education and sites and materials accessed must be appropriate to work in school.
9. All e-mails sent and received will be virus checked and electronically read for content but it is each user's responsibility to ensure that acceptable levels of language and content are used at all times.
10. Legitimate private interests may be followed providing school use is not compromised but use for personal gain, purchasing, gambling, and political purposes or for advertising is forbidden.
11. The school follows the B&NES "e-mail and Internet Access – User Guidelines" and the B&NES "e-mail and Internet Policy".
12. Laptop computers can be used in a wireless environment and for further information and documentation, consult ICT Technical Support or the school web-site.
13. Tampering with any of the school's ICT equipment be it physically, electronically or changing of settings, is a serious offence and as such will be treated accordingly in line with the school's behaviour policy.
14. The school reserves the right to remove any of network, Internet or e-mail access from any member of staff or student who is found to be in breach of this policy.
15. Each student's basic data is held on our administration computer system and as such it is shared with our careers service with a view to helping students with future employment and/or further education.
16. The school has a web-site and on occasions it will contain the names of students associated with school activities and work. It may also contain photos of students but it is our intention not to place both names and images in the same article.
17. Users must not attempt to access restricted portions of the network, an operating system, security software or other administrative applications without appropriate authorisation by the system administrator.
18. Users must not use school's computing and/or network resources in conjunction with the execution of programs, software, processes, or automated commands that are intended to disrupt (or that could reasonably be expected to disrupt) other computer or network users, or damage or degrade performance, software or hardware components of a system.

D. Fair Share of Resources

The ICT Support department which operates and maintains computers, network systems and servers, expects to maintain an acceptable level of performance and must assure that senseless, excessive, or inappropriate use of the resources by one person or a few people does not degrade performance for others. The school network, computer suites, the Library and other central computing resources are shared widely and are limited, requiring that resources be utilised with consideration for others who also use them. The school may choose to set limits on an individual's use of a resource through quotas, time limits, and other mechanisms to ensure that ICT resources can be used by anyone who needs them.
If any student, member of staff, parent or carer is unsure about any of the above, or for further clarification, they are to consult Mr J Webber, Head of ICT; Mr D Lagoudakis, Network Manager; or Mr C Hildrew, Deputy Headteacher.

Appendix 3

Student Acceptable Use Policy

1. Rationale

1.1 This summarises the key responsibilities and required behaviour of all students towards the computer and information systems of Chew Valley School.
The school assumes that parents will ensure that their child reads this policy before coming to school in September.

1.2 This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communication technologies for educational, personal and recreational use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

2. Policy

2.1 Users are encouraged to make use of the school's computing facilities for educational purposes. All users are expected to act responsibly and to show consideration to others. All students are required to adopt procedures and practices that ensure the security, integrity and protection of information created and held by Chew Valley School, and to abide by the school's rules for the use of computer systems.

2.2 Rules for the Use of school's Computer Equipment:

- You must not remove computer equipment from the school without permission from the Network Manager.
- You must not install unlicensed software or applications on the school's computers, servers, laptops or mobile devices.
- You must not bypass any security measures put in place to ensure the safe operation of computing equipment, information systems or communications equipment e.g. disabling anti-virus software, removing password protections etc.
- You may only access, modify, save or copy records or files and computer records where you have been given the authority and authorisation to do so.
- You must not connect equipment to the school's wired network without permission from the Network Manager.
- If you discover a security problem, for example being able to access other users' data, you must inform the Network Manager immediately and not show it to other users. Students identified as a security risk will be denied access to the network.

3. Mobile Devices Code of Conduct

- Portable devices include, but are not limited to: Laptops, Tablets and Netbooks.
- Students using school portable devices are expected to act in a responsible, ethical and legal manner in accordance with the acceptable use policy.
- Students are responsible for inspecting and reporting malfunctions of hardware and software at the beginning and end of each usage.
- Portable devices should never be left unattended.

- Portable devices should never be taken out of School unless directed by a teacher.
- Portable devices are delicate electronic equipment and require care to ensure proper operations.
- No software/apps are to be downloaded or installed onto a mobile device or computer without permission from the classroom teacher or the Network Manager.
- The use of any portable device must support education and research and adhere to the educational goals of Chew Valley School.

Appendix 4
Social Media Policy

1. Rationale

1.1 The widespread availability and use of social media applications bring opportunities to understand, engage, and communicate in new and exciting ways. It is important that we are able to use these technologies and services effectively and flexibly. However, it is also important to ensure that we balance this with our duties to our school, the community, our legal responsibilities and our reputation. For example, our use of social networking applications has implications for our duty to safeguard children, young people and vulnerable adults.

1.2 The policy requirements in this document aim to provide this balance to support innovation whilst providing a framework of good practice. They apply to all members of staff at the school. The purpose of the policy is to:

- Protect the school from legal risks.
- Ensure that the reputation of the school, its staff and governors is protected.
- Safeguard all children.
- Ensure that any users are able clearly to distinguish where information provided via social media is legitimately representative of the school.

2. Definitions and Scope

2.1 Social networking applications include, but are not limited to: Blogs, Online discussion forums, Collaborative spaces, Media sharing services, 'Microblogging' applications, and online gaming environments. Examples include Twitter, Facebook, Windows Live Messenger, YouTube, Flickr, Xbox Live, Blogger, Tumblr, Last.fm, and comment streams on public websites such as newspaper site.

2.2 Many of the principles of this policy also apply to other types of online presence such as virtual worlds.

2.3 All members of staff should bear in mind that information they share through social networking applications, even if they are on private spaces, are still subject to copyright, data protection and Freedom of Information legislation, the Safeguarding Vulnerable Groups Act 2006 and other legislation. They must also operate in line with the school's Equalities, Child Protection and ICT Acceptable Use Policies.

2.4 Within this policy there is a distinction between use of school-sanctioned social media for professional educational purposes, and personal use of social media.

3. Use of Social Media in practice

3.1 Personal use of social media:

- School staff must not invite, accept or engage in communications with parents or children from the school community in any personal social media whilst in employment at Chew Valley School.
- Any communication received from children on any personal social media sites must be reported to the designated person for Child Protection (Deputy Headteacher, Pastoral).

- If any member of staff is aware of any inappropriate communications involving any child in any social media, these must immediately be reported as above.
- Members of the school staff are strongly advised to set all privacy settings to the highest possible levels on all personal social media accounts.
- All email communication between staff and members of the school community on school business must be made from an official school email account.
- Staff should not use personal email accounts or mobile phones to make contact with members of the school community on school business, nor should any such contact be accepted, except in circumstances given prior approval by the Headteacher.
- Staff are advised to avoid posts or comments that refer to specific, individual matters related to the school and members of its community on any social media accounts.
- Staff are also advised to consider the reputation of the school in any posts or comments related to the school on any social media accounts.
- Staff should not accept any current student of any age or any ex-student of the school under the age of 18 as a friend, follower, subscriber or similar on any personal social media account.

3.2 School-sanctioned use of social media

3.2.1 There are many legitimate uses of social media within the curriculum and to support student learning. For example, the school has an official Twitter account (@ChewValleySch), and several A-level courses require the use of blogs for assessment. There are also many possibilities for using social media to enhance and develop students' learning.

3.2.2 When using social media for educational purposes, the following practices must be observed:

- Staff should set up a distinct and dedicated social media site or account for educational purposes. This should be entirely separate from any personal social media accounts held by that member of staff, and ideally should be linked to an official school email account.
- The URL and identity of the site should be notified to the appropriate Head of Faculty or member of the SLT before access is permitted for students.
- The content of any school-sanctioned social media site should be solely professional and should reflect well on the school.
- Staff must not publish photographs of children without the written consent of parents/carers, identify by name any children featured in photographs, or allow personally identifying information to be published on school social media accounts.
- Care must be taken that any links to external sites from the account are appropriate and safe.
- Any inappropriate comments on or abuse of school-sanctioned social media should immediately be removed and reported to a member of SLT.
- Staff should not engage with any direct messaging of students through social media where the message is not public.
- All social media accounts created for educational purposes should include a link in the About or Info page to the ICT Acceptable Use Policy on the school website. This will indicate that the account is officially sanctioned by Chew Valley School.