Date: Autumn 18

E-Safety Policy

WATCOMBE PRIMARY SCHOOL

TORBAY COUNCIL

E-Safety Policies and Procedures

WATCOMBE PRIMARY SCHOOL

Name of Policy:

E-Safety Policy and Procedures

This policy was adopted by the Children and Curriculum Committee at their meeting:

Spring Term 2016

E-Safety Policy

Background and Rationale

First and foremost e-Safety, as with all safeguarding matters, is about keeping children safe and our fundamental responsibility to ensure that this happens. The Watcombe School community, including all its stakeholders, recognises the importance of taking e-Safety and the need to keep this ever-developing area of technology under review. In a nutshell, when it comes to e-Safety, E is for Everyone.

Creating a safe ICT learning environment

Protecting young people (and adults) properly means thinking beyond the traditional school environment. Where once the desktop computer was the only way to access the internet, now many mobile phones and games consoles offer broadband connections. Our pupils may be working online in school, at home or in an internet cafe. They may have personal devices not covered by network protection and therefore the emphasis must be on getting everyone to understand the risks and act accordingly. This has four important elements:

an infrastructure of whole-site awareness, responsibilities, policies and procedures

an effective range of technological tools

a comprehensive e-safety education programme for everyone in our establishment a review process which continually monitors the effectiveness of the above.

It must be clearly understood that e-safety is a **child safety** (not an ICT) issue, and indeed it should not be managed primarily by the ICT team (Subject Leader & HLTA). It should be an extension of general safeguarding, for instance, cyber bullying is considered alongside real-world bullying

In treating e-Safety as an ever-present potential danger, aspects of e-Safety are implicit in all aspects of our ICT and safeguarding policies and procedures throughout the school.

This policy links all the ICT, safeguarding and other policies and procedures that explain how the school deals with e-Safety issues.

The policy reflects of the importance of the procedures and practices that need to go on across the school every day.

Development, Monitoring and Review

The documents referred to in this e-Safety policy have been developed through consultation with and between:

- The Headteacher
- Senior Leadership Team
- Designated Child Protection staff
- ICT Specialist HLTA
- Teachers

- Support Staff
- Governors
- Parents and Carers
- Pupils

An e safety group will oversee the E safety across the school as part of the SSE. This group will comprise of: HT, ICT subject Leader, ICT HLTA and an appointed governor.

The e-Safety Policy will be reviewed termly and formally adopted annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to eSafety or incidents that have taken place.

N.B. Other associated policies that form appendices to this document will be updated as and when the substantive policies are reviewed

Should serious e-Safety incidents occur, the following people and agencies should be informed:
Designated Safeguarding Lead in school
LA Safeguarding Officer

A serious incident is one where a child has suffered or is likely to suffer significant harm including incidents when they are being exploited on-line.

The school will monitor the impact of the policy using:

- Logs of reported incidents
- SWGfL monitoring logs of Internet activity (including sites visited)
- Surveys / questionnaires of pupil, parents, carers and staff
- Annual review of E safety using the 360 review programme

Scope of the Policy

This policy applies to all members of the school community (including staff, pupils, students, work experience, volunteers, parents and carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school.

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other e-Safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

The school will deal with such incidents within this policy and associated behaviour and antibullying policies and will, where known, inform parents or carers of incidents of inappropriate e-Safety behaviour that take place out of school.

Roles and Responsibilities

Mobile phones should not be used in any classroom or area where there are children (unless by prior arrangement with the HT or DHT). Mobile phones can only be used in office space or the staffroom.

The following section outlines the roles and responsibilities for e-Safety of individuals and groups within the school:

Governors:

- Governors are responsible for the approval of the e-Safety Policy documents and for reviewing the effectiveness of the policy. As users of our ICT systems they are also subject to those policies and procedures.

Senior Leadership Team & ICT Specialist HLTA:

- The Headteacher is responsible for ensuring the safety (including e-Safety) of members of the school community.
- The Headteacher, members of the Senior Leadership Team must be aware of the procedures to be followed in the event of a serious e-Safety allegation being made against a member of staff. This is defined as „Serious Allegation Made Against a Member of Staff; E-Safety"
- Takes day to day responsibility for e-Safety issues and has a leading role in establishing and reviewing the school e-Safety policies and documents.
- Manages all permissions documentation and the Upper School pupil"s Acceptable use Policy (AUP)
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-Safety incident taking place as detailed in the **e-Safety Child Protection Protocol**
- Provides training and advice for staff
- Liaises with the ICT network group.
- Liaises with school ICT technical staff
- Reports regularly to Senior Leadership Team
- That the school"s ICT infrastructure is secure and is not open to misuse or malicious attack
- That the school meets the e-Safety technical requirements outlined in the SWGfL Security Policy and Acceptable Usage Policy and any relevant Local Authority e-Safety policy and guidance
- Users may only access the school"s networks through a properly enforced password protection policy, in which passwords are regularly changed
- That no filters are removed without the authorisation of the e-Safety Team who will ensure that all implications are considered including contact with SWGfL to ascertain the reason for filtering
- SWGfL is informed of issues relating to the filtering applied by the Grid

Designated Persons for Child Protection

The Designated Persons should be trained in e-Safety issues and be aware of the potential for serious child protection issues to arise from:

- sharing of personal data and their vulnerability to "web crawlers"
- access to illegal and inappropriate materials and websites e.g. that promote diet plans that are age inappropriate and could lead to eating disorders
- inappropriate on-line contact with adults including strangers
- potential or actual incidents of grooming
- sexting, where personal photographs of a sexual nature are attached to text messages
- cyber-bullying

Teaching and Support Staff

Teaching and support colleagues are responsible for ensuring that:

- they follow the requirements of their AUP
- they have an up to date awareness of e-Safety matters and of the current school e-Safety policy and practices
- they have read, understood and signed the school Staff Acceptable Use Policy (AUP)
- they password protect their laptop and classroom computer
- they report any suspected misuse or problem to the Headteacher for investigation, action or sanction
- digital communications with pupils / parents should only be on a professional level and only carried out using official schoolsystems. When a member of staff leaves the school such communications should cease.
- pupils understand and follow the school e-Safety and acceptable use policy.
- older pupils are introduced to the need to avoid plagiarism and uphold copyright regulations
- they monitor ICT activity in lessons, extra curricular and extended school activities
- they are aware of e-Safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices
- In lessons, where Internet use is pre-planned Lower School pupils should be guided to sites checked as suitable for their use. To facilitate a more independent approach to the gathering of information, from Y2 upwards this process is not used but there is a focused procedure in place for guiding pupils in dealing with any unsuitable material that is found in Internet searches

- Teachers may wish to use teaching resources from filtered websites such as You tube. Each teacher must take responsibilities for using this safely and ensure that no searches, other than those carried out by themselves, can be accessed.

  WARNING – YOUR ARE RESPONSIBLE FOR CLOSING DOWN YOUR INTERNET WINDOW AFTER USE IN THE CLASS. **DO NOT LEAVE IT OPEN** AS THIS WILL ALLOW ANY USERS FREE ACCESS OF THE INTERNET. THE COMPUTER MUST NOT BE LEFT UNATTENDED.

- The webpage details (URL) of any inappropriate sites accessed are emailed to the ICT Specialist HLTA for immediate blocking.

Pupils:

- Are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy, which they will be expected to sign before being given access to school systems (at the beginning of KS1 & again at the start of KS2)

Should have an age appropriate understanding of research skills and the need to avoid plagiarism and uphold copyright regulations. This is part of our curriculum input and their skills will be supported through active teaching.

- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so. They will be reminded before every occasion they use ICT tools and equipment independently.
- Will be expected to know and understand school policies on the use of mobile phones, personal digital cameras and mobile devices. They should also know and understand school policies on the use of images and on cyber-bullying. This is part of the curriculum and understanding of this requirement will be assessed, supported and followed up if a deliberate breach occurs.
- Should understand the importance of adopting good e-Safety practice when using digital technologies out of school and realise that the school"s e-Safety Policy covers their actions out of school, if related to their membership of the school. Pupils and parents will receive guidance on the importance of safe practice and we shall use all our monitoring technologies where possible.

Parents and Carers

Parents and carers play a crucial role in ensuring that their children understand the need to use the Internet and mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through parents" evenings, newsletters, letters, website and information about both national and local e-Safety campaigns and literature. Parents and carers will be responsible for endorsing (by signature) the Pupil Acceptable Use Policy.

At school events (Christmas plays, assemblies etc) parents are asked to focus upon their children only. If other children are in the photo they are requested not to post these on to social network sites.

Policy Statements

Education – pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in 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. **A key emphasis for us is to empower pupils to protect themselves.**

e-Safety education will be provided in the following ways:

- A planned e-Safety programme will be provided as part of ICT curriculum identified as Core ICT Skills on our annual planning cycle and will therefore be taught throughout the year to all pupils across the school year – this will cover both the use of ICT and new technologies in school and outside school. This is delivered through specific blocks of work and continuously referred to whilst using ICT.

- Key e-Safety messages should be reinforced as part of Team assemblies and pastoral activities
- Pupils will be reminded on a regular basis in lessons to be critically aware of the materials and content they access on-line and be guided through discussion to recognise that not all information found online is accurate
- Pupils should be helped to understand the need for the Pupil Acceptable Use Policy and encouraged to adopt safe and responsible use of ICT, the Internet and mobile devices both within and outside school.
- Rules for use of ICT systems and safe Internet use will be displayed in ICT Suites and computer areas.

Education – parents and carers

The school seeks to provide information and awareness to parents and carers through:

- Letters, newsletters, web site
- Parents evenings
- Reference to the SWGfL Safe website (noting the SWGfL "Golden Rules" for parents)

Education and Training – Staff

All staff receive e-Safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal e-Safety training will be made available to staff. An audit of the e-Safety training needs of all staff will be carried out regularly.
- All new staff will receive e-Safety training as part of their induction programme, ensuring that they fully understand the school e-Safety policy and Acceptable Use Policies
- The ICT Specialist HLTA & Designated teachers will receive regular updates through attendance at appropriate training sessions and by reviewing guidance documents released by BECTA, SWGfL, the LA, LSCB and others.
- The ICT Specialist HLTA will provide advice, guidance and training to individuals as required.

Training – Governors

Governors will receive regular information updates on e-Safety training and monitoring. In addition they will receive training as part of their annual CPD provision.

Technical – Infrastructure, Equipment, Filtering and Monitoring

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

- School ICT systems will be managed in ways that ensure that the school meets the e-Safety technical requirements outlined in the SWGfL Security Policy and Acceptable Usage Policy and any relevant Local Authority E-Safety Policy and guidance
- There will be regular; at least annual, reviews and audits of the safety and security of school ICT systems and in addition this will be triggered should an incident occur when e-Safety is compromised

- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded and managed by the ICT Specialist HLTA and will be reviewed, at least annually, by the e-Safety Committee.
- All adult users will be provided with a username and password by the ICT Specialist HLTA.
- The Administrator passwords for the school ICT system must be available to the Headteacher and kept in a secure place (School safe).
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security to the ICT Specialist HLTA

- ~~The school maintains and supports the managed filtering service provided by SWGfL~~
- Any filtering issues should be reported immediately to SWGfL.
- The filtering provider (SWGfL) regularly monitor and record the activity of users on the school ICT systems and users are made aware of this.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.
- An agreed policy is in place in the AUP regarding the downloading of executable files. This can only be done by ICT Specialist HLTA in line with advice from the technical support team.
- An agreed policy is in place in the Staff Laptop Policy regarding the extent of personal use that users and their family members are allowed on laptops and other portable devices that may be used out of school. We believe that confidence comes from regular use and encouraging personal activity is a good way to ensure that. Essentially it is acceptable to use laptops for personal use provided that only appropriate information and websites are accessed and no illegal activity is undertaken whilst using them. It is also essential that laptops are encrypted and password protected in case of theft
- The school infrastructure, individual workstations and all laptops are protected by up to date virus software. We ask that all staff ensure that personal computers, not owned by the school, are also protected by up to date virus software to protect any virus contamination.
- Personal data cannot be sent over the Internet or taken off the school site unless safely encrypted or otherwise secured. This includes any data related to staff or pupils.
- Data pens are not permitted to be used to transfer files between computers unless they have been scanned **immediately beforehand** to prevent spreading viruses. Alternatively colleagues may wish to email files or load them onto the Shared Area. Such is the potential

to cause critical damage to our systems that failure to comply with this requirement may lead to formal action being taken.

Curriculum

E-Safety should be a focus in all areas of the curriculum and staff should reinforce eSafety messages in the use of ICT across the curriculum.

- In lessons where Internet use is pre-planned using specific online resources, it is best practice that those sites should be checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in Internet searches.
- Where pupils are allowed to freely search the Internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites pupils visit. In this context it is essential that pupils are clear as to what to do if they access something inappropriate; turn off the monitor and go quietly to an adult and tell them. The adult will then take a note of the website address and the route taken to get there. This is often through search engines. Once this is done, note the number of the desktop, close the Internet session and restart it instructing the pupil that they must not seek to access the site again. Adults to report appropriately
- Any infringement of the Pupil AUP will result in that pupil being spoken to by the ICT Specialist HLTA and if there is any further infringement this will result in them being denied access to the Internet and the matter will be recorded and reported to the Headteacher for appropriate action.

- It is accepted that from time to time, for good educational reasons, sites filtered by SWGfL result in Internet searches being blocked. This is particularly frustrating when good learning resources are made unavailable. In such a situation, staff can request that the ICT Specialist HLTA can permanently or temporarily remove those sites from the filtered list. Any request to do so, should be auditable, with clear reasons for the need and only after sanctioning by the e-Safety Team and thorough investigation can any site be unfiltered.
- Pupils should be taught in all lessons to be critically aware of the materials and content they access on-line and be guided to consider the accuracy of information
- All pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the Internet.

Use of digital and video images – Photographic and Video

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images in an appropriate way. This is applicable to pupils in Key Stage 2, many of whom are already on social networking sites, despite the fact that they are significantly below the age limit. In particular pupils should recognise the risks attached to publishing their own images on the Internet e.g. on these social networking sites.
- Staff are allowed to take digital and 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, including mobile phones, should not be used for such purposes without permission from the Headteacher.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils" full names will not be used anywhere on a website or blog, particularly in association with photographs.
- We maintain a list of pupils whose parents do not wish their image to appear beyond the school. Staff need to refer to this list, issued to them at the beginning of each academic year.These pupils will not have any photograph of them, face-on, published in any way. Photographs may be used in classrooms.
- We are sometimes called upon to make films or publications for external organisations that include pictures of our pupils. In such circumstances, parental permission is required and a copy of the permissions form is in the appendices of this document.

Data Protection

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.

Staff must ensure that they comply with the Data Policy by:

- At all times taking care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Using personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transferring data using encryption and secure password protected devices.

Communications

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

- The official school email service may be regarded as safe and secure and is monitored.
- Users need to be aware that email communications may be monitored
- Users must immediately report, to the Headteacher, in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and pupils or parents or carers (email, chat, VLE etc) must be professional in tone and content.

Unsuitable or Inappropriate Activities

The school believes that the unacceptable activities referred to in the AUP would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems.

Responding to incidents of misuse

N.B. If any apparent, suspected or actual misuse appears to involve illegal activity i.e.

- child sexual abuse images
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

The School Protocol on Child Protection and e-Safety Protocol must be followed.

Appendices

The following policies can be found in the Staff Shared Area:

For Staff : All school policies

For Governors: Governors Area – All school Policies

Appendix 1: Pupil Acceptable Usage Policy
Appendix 2: School Filtering Procedure
Appendix 3: School Password Procedure

Appendix 4: Software Compliance and Administration Network Security Policy
Appendix 5: Staff Laptop and Data Usage Policy

Appendix 6: Child Protection Policy (including the Internet Safety
Protocol) Appendix 7: Anti Bullying Statement

Pupil ICT Agreement (Acceptable Use Policy):

Appendix 1

We allow you to use our School ICT Network and the different programs that are there to help you with your learning. It also allows you to go onto the Internet. We trust you to use these programs and the Internet safely and sensibly.

Here is important information you must know:

- Your folders belong to the school and staff will look at the files in there. They are not private to you.
- Staff can see what you are doing on a computer at any time and can track what you have been doing after you finish.
- The use of the Internet is a privilege and provided for your learning. All the sites you visit are recorded.
- Not everything you find on the Internet is true.
- There are people on the Internet who might try to use any information you give them to hurt you and all the rules we have are there to keep you safe. That is why it is important to follow them.

There are pictures and text on the Internet that are so nasty you would not want to see them and we try to keep those sites away from you. Sometimes they get around our safety system and if they do we expect you to turn off the monitor and quietly tell an adult. You must not show what you have seen to another pupil or ever try to return to that site.

- Mobile phones, personal cameras and other portable devices are not allowed in school and should be handed into the office for safe keeping during school hours.

Here are the rules you must follow:

- We expect you to behave sensibly and safely whilst using ICT equipment.
- Treat any computer of piece of ICT equipment with respect so that it does not get damaged. You should not move any equipment unless a member of staff asks you to and you should never touch plugs or leads. The School reserves the right to seek payment from parents of pupils who cause malicious damage to ICT equipment.
- You must only use your log on.
- Use only appropriate sites that can be accessed via the school website.
- **If you do any of the following things in school, on purpose, you will be reported to the Headteacher and we will prevent you from using the Internet and contact your parents:**
- Visiting Internet sites without permission.
- Trying to access sites that have nasty images or material.
- Using someone else"s log on and going into their personal folder.

Please sign to say that you agree to follow these rules and return the slip below to school:

I agree to abide by the rules of the „Watcombe Primary School Pupils" ICT Agreement".

Pupil Name ______________________ Class __________ __________

Pupil signature ______________________ Date __________

Parent signature in support ______________________ Date __________

Pupil Acceptable Usage Policy: This is reviewed on an annual basis.

Appendix 2

School Filtering Procedure

Introduction

The filtering of Internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so. It is therefore important that the school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.

As a part of the South West Grid for Learning (SWGfL), Watcombe School automatically receives the benefits of a managed filtering service, with some flexibility for changes at local level.

Responsibilities

It is the responsibility of all users to comply with the Acceptable Use Policy and the Child Protection Internet Protocol.

Monitoring

No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network and on school equipment as indicated in the Acceptable Use agreement. Monitoring will take place by regular checking of key words.

If inappropriate material is accessed the user must follow the AUP guidelines. The ICT Specialist HLTA will log this appropriately and then filter the site. SWGfL will be contacted if the problem persists.

Audit and Reporting

Logs of filtering change controls and of filtering incidents will be made available to the Headteacher and Governing Body

Proxy settings for the HT and DHT machines enable access to the wider range of sites but still protected by the base filter.

Users of such machines are subject to a termly internet usage check.

Cameras are sited in shot of the CCTV.

Appendix 3

School Password Procedure

Introduction

The school will be responsible for ensuring that the school infrastructure is as safe and secure as is reasonably possible and that:

- users can only access data to which they have right of access
- no user should be able to access another‟s files, without permission (or as allowed for monitoring purposes within the school‟s policies).
- access to personal data is securely controlled in line with the school‟s personal data policy
- logs are maintained of access by users and of their actions while users of the system

A safe and secure username and password system is essential if the above is to be established and will apply to all school ICT systems, including email and Virtual Learning Environment (VLE).

Procedure

All passwords are generated by the ICT Specialist HLTA.

- All teaching staff have access to Student files.
  Passwords can only be reset by the ICT Team
- All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the ICT Specialist HLTA and will be reviewed annually.
- The administrator passwords for the school ICT system is kept in a secure place (school safe).
- In the event of a serious security incident, the police may request and will be allowed access to passwords used for encryption (school safe).

Appendix 4

Software Compliance and Administration Network Security Policy

Introduction

To ensure that all software (both Operating Systems and Applications) is correctly licensed and recorded the following procedure must be followed:

- Budget plans for new or replacement hardware must include a revenue provision for all required licences or upgrades.
- Care must be taken that any licences, including licence subscriptions, must be budgeted.
- The ICT Specialist HLTA will maintain a full database of all software in use within Watcombe School. Original licences for software will be kept the school safe.
- Where free software is provided by the Government, DCSF, or various other bodies, a copy of the letter or remittance advice, must be given to the ICT Specialist HLTA so that the software is logged. Even when it is license free, the ICT Specialist HLTA is still responsible for overseeing the loading and maintenance of all software on both the Curriculum, Laptops for Teachers and Admin systems (SIMs applications on the Administration system will be overseen by Scomis as part of our contract.

- Where any concern about software usage is raised, the ICT Specialist HLTA will provide the Headteacher with requisite records.

If any colleague has any concerns or queries about the Watcombe compliance policy they should raise these with either the ICT Specialist HLTA who will be more than happy to help.

Administration Network Security Policy

The system management comprises of:

- Personnel & Finance Administrator

The school's accounting system is computerised and access to the accounting records is restricted to authorised staff and the LA.

All access rights must be authorised by the Headteacher and then actioned accordingly by the Personnel & Finance Administrator ensuring confidentially at all times. The system is accessed by passwords, which are regularly changed in line with ICT policy. They are changed immediately if an employee is aware that an unauthorised person has learnt their password.

The system is automatically backed-up daily, to a remote location at Scomis in Exeter.

Systems are in place in line with ICT policy to safeguard school software and data against computer viruses.

The school complies with the requirements of the Data Protection Act.

Appendix 5

Staff Computer Acceptable Use Policy

This policy is reviewed annually or as necessary

- I will only access the system with my own name and registered password, which I will keep secret. I will inform the ICT HLTA as soon as possible if I know my password is no longer secret. Personal passwords must be registered with the ICT HLTA and up dated if changed. (These will be stored in a secure place)
- I acknowledge that the computer provided for me to use remains the property of Watcombe School and should only be used for appropriate activities and tasks.
- I will not access the files of others or attempt to alter the computer settings.
- I will not update web logs or use pictures or text that can identify the school, without the permission of the Headteacher.
- I will not alter, attempt to repair or interfere with the components, software or peripherals of any computer that is the property of Watcombe School.
- I will always log on using my password and log off the system when I have finished working.
- I understand that the school may, in line with South West Grid for Learning/DfE policy, check my computer files and e-mails and may monitor the Internet sites I visit.
- I will always adhere to the Watcombe E - Safety Policy.
- I will not open e-mail attachments unless they come from a recognised and reputable source. I will bring any other attachments to the attention of the ICT HLTA.
- Any e-mail messages I send will not damage the reputation of the school.
- Any joke e-mails and attachments should be considered carefully before being forwarded to ensure that they do not contain any offensive, illegal or virus content. If in any doubt they should not be sent.
- I will report immediately, to the Headteacher, any unpleasant material or messages sent to me.
- Posting anonymous messages and forwarding chain letters is forbidden.
- I understand that a criminal offence may be committed by deliberately accessing Internet sites that contain certain illegal material.
- Use for personal financial gain, gambling, political purposes or advertising is forbidden.
- Storage of e-mails and attachment should be kept to a minimum to avoid unnecessary drain on memory and capacity

- Activity that threatens the integrity of the school ICT systems, or activity that attacks or corrupts other systems, is forbidden.
- I understand that I am responsible for the safety of sensitive school data that I use or access.
- In order to maintain the security of data I will take the following steps:

- I will store data files in my user area only for as long as is necessary for me to carry out my professional duties. Photographs must be stored to an archive at the end of a year.
- I will not save data files to a PC or laptop other than that provided by the school.
- I will not share or give out any passwords that I use to access school systems – if I have reason to believe that my password is no longer secure I will seek to change it.
- Where possible I will transfer files by saving them to the school network area if other staff need access to the information.

Sensitive data could include:

- Pupil reports
- SEN records
- Letters to parents
- Class based assessments
- Exam results
- Whole school data
- Medical information
- Information relating to staff, e.g. Performance Management reviews.

If you are in any doubt as to the sensitivity of data you are using, please consider these questions:

- Would it place anyone at risk?
- Would it cause embarrassment to an individual or the school?
- Would it have legal or financial implications?

If the answer to any of these questions is yes, then please treat the data as sensitive.

- I understand that if I do not adhere to these rules outlined in this policy, my network access may

be suspended immediately, my laptop removed and that other disciplinary consequences may follow.

NBPlease also refer to the Software Compliance Policy.

Name

Signature Date

Authorisation:**Date**:

Appendix 6

Child Protection and Internet Safety Protocol at Watcombe School (Addendum to Child Protection Policy)

The most important and effective strategy to keep children safe is education.Through the e-Safety curriculum, discussion, support and guidance by staff, and support to parents, we can equip pupils with the skills and attitudes to keep themselves safe and avoid risk taking behaviour. This is the single most important task we undertake when considering eSafety as every system has its failures but applying common sense, simple rules and being prepared for taking the appropriate action whilst looking to trusted adults for support, is by far the best way to stay safe.

Here are some of the ways we use systems to help:

The Internet is provided by SWGfL, which has a range of filters and security devices. Every time pupils log on they agree to the School"s Internet Use Policy.However, some problems can still arise. These are most commonly that:

Pupils find inappropriate images and/or language on sites that they have found in the course of their work. In this case the teacher needs to:

- Record the name of the student, the web address and the machine they were on e.g. IT Zone 1, Machine 4).
- Pass this information on to the ICT HLTA.
- The ICT HLTA will then notify the SWGfL so the site can be filtered or if it is an image on a site it will be filtered directlyand let the Headteacher know if there any child protection issues through the usual procedures. This will then be logged.

If the teacher feels these images have been saved into the pupil"s work area they should inform the ICT HLTA. They will then go into the pupil"s work area and retrieve then delete the image. This will be reported to the Headteacher who will take appropriate action.

There may be instances when teachers need to do searches and accidentally go to web pages that may contain inappropriate images. If this happens they must notify the ICT HLTA so the use can be filtered and recorded.

If there are <u>any</u>concerns raised, no matter how small CP Designated Officers should be informed immediately and they may decide to make a referral to Children"s Services.

Appendix 7

Anti-Bullying Statement

This policy is reviewed annually

Respect is a Core Value at Watcombe School. We have high expectations of the way that pupils and adults interact within and between those groups. Adults are all expected to provide the highest standard of role modelling and we pride ourselves that we do so. We expect everyone to respect each other and behave in a respecting way.

Watcombe School is also a „Telling School". We encourage pupils to tell adults if they are unhappy with the behaviour of another pupil towards them and we encourage parents to contact the class teacher if inappropriate behaviour has occurred and the Headteacher if they are concerned that repeated incidents have occurred that may be viewed as bullying.

The aim of our anti-bullying policy is to clarify for pupils and staff that bullying is unacceptable. We wish to encourage an environment where independence is celebrated and individuals can flourish without fear. Every student has the right to be safe and happy in school and to be protected when they are feeling vulnerable.

All reports are treated seriously and discretely. The Headteacher meets with all those involved and works with them to change behaviours.

What is Bullying?

Bullying is the repeated use of any behaviour intended to hurt another person, resulting in pain and/or distress.

There are many different forms of bullying including:

Physical - hitting, kicking, spitting and damaging belongings Verbal -
name calling, insults, spreading rumours or teasing

Emotional - exclusion

Cyber -sending unkind and offensive electronic messages by text, email, websites or socialnetworking sites

If a pupil is unhappy with the way that an adult has behaved towards them they are encouraged to speak to another adult they trust so that the matter may be referred to the Headteacher to be investigated and addressed in a way that is open and fair to all those involved. Further details about our anti-bullying policy can be accessed via the school website.