E-Safety Policy

Article 3 – The best interests of the child must be a top priority in all things that affect children.

Article 16 – Every child has the right to privacy. The law should protect the child's private, family and home life.

Article 29 – Education must develop every child's personality, talents and abilities to the full. It must encourage the child's respect for human rights, as well as respect for their parents, their own and other cultures, as well as the environment.

Nova Primary School Governor Information	
Model Policy	Yes
Local Changes	
Customisation*	
Originally Adopted	Spring 2010
Last Review Date	Spring 2019
Next Review Date	Spring 2020
* additions made to policy (eg local detail) but not a change to any policy structure	

History of most recent policy changes – Must be completed

Date	Page	Change	Origin of change e.g. TU request, change in legislation
27.02.13	1	Addition of children's rights	
17.01.13	13	Online search engine platform added	
10.10.14	1	Training dates added	
28.11.14	Various	Updating e-safety procedures at Nova Primary School. Links with the new curriculum guidance as of Sept 2014. Date of the policy – 2014	
28.11.14	4	Technician details for reporting	
May 2015	Various	Updated to reflect current guidelines and changes in documentation within school	
January 2018	Various	Links updated and changed. Logging e-safety incidents is now done on CPOMS. Added Cyber bullying section.	
January 2018	9	Changed timeframe of holding children's photographs on the server.	
January 2018	10	Extended paragraph about the way in which e-safety is taught	
January 2018	17	Added in how we take part in internet safety day	
January 2019	Various	Removed Swiggle search engine section and given updated advice for using search engines. Updated advice on supervision of internet access by staff members only.	
July 2019	Various Page 13 Page 18	Added to section 8 regarding online presence and updated guidance from DFE. Section on vulnerable pupils added in response to updated guidance from DFE Added links to some further resources from DFE	

Contents

1. Core Principle of Internet Safety
2. Use of the Internet
3. Enhancing Learning Through the Internet
4. Authorised Access to the Internet
5. Filtering
6. Assessing Risks and Monitoring
7. Managing Content
8. Online Communications and Social Networking
9. Mobile Technologies
10. Cyber bullying
11. Vulnerable pupils
12. Pupils Knowledge of the E-Safety Policy
13. Parents
14. Staff
15. Complaints
16. E-Safety Logging Procedure

Appendix 1 – Pupil's Acceptable and Responsible Internet Use

Appendix 2 – Web Based Resources

Appendix 3 – Notes on the Legal Framework

Appendix 4 – Glossary of Terms

Context

Nova Primary School enjoys a modern state-of-the-art computing and networking infrastructure. We have strong ICT leadership and a strong emphasis on the pervasive use of ICT equipment as part of the curriculum taught to all pupils and how this can be applied in all subjects.

There are risks associated with the use of ICT equipment that will face pupils at school and at home. Yet, a working knowledge of how to apply ICT equipment is vital to the future prospects of our pupils. For that reason, e-safety is an integral part of ICT education at Nova Primary School.

Nova Primary School aims to create pupils who are educated, responsible, and safe digital citizens for their life at school, at home and for their future. The purpose of this policy is to guide these aims.

1. Core Principles of Internet Safety

The internet is becoming as commonplace as the telephone or television and its effective use is an essential life skill. Unmediated internet access brings with it the possibility of placing pupils in embarrassing, inappropriate and even dangerous situations. Schools need a policy to help ensure responsible usage and the safety of pupils.

Nova Primary School's E-Safety Policy is built on the following five e principles of the Bristol City Council E-Safety Policy and informed by Ofsted documents:

<u>Guided Educational Use</u>

Significant educational benefits should result from curriculum internet use including access to information from around the world and the ability to communicate widely and to publish easily. Curriculum internet use should be planned, task-orientated and educational within a regulated and managed environment. Directed and successful internet use will also reduce the opportunities for activities of dubious worth.

<u>Risk Assessment</u>

21st century life presents dangers including violence, racism and exploitation from which children and young people need to be protected. At the same time they must learn to recognise and avoid these risks by becoming 'internet wise'. Schools need to ensure that they are fully aware of the risks,

perform risk assessments and implement a policy for internet use. In addition, pupils need to know how to cope if they come across inappropriate material.

Pupils may obtain internet access in youth clubs, libraries, public access points and in homes. Ideally a similar approach to risk assessment and internet safety would be taken in all these locations, although risks do vary dependent on the situation.

Responsibility

Internet safety depends on staff, schools, governors, advisers, parents and, where appropriate, the pupils themselves taking responsibility for the use of internet and other communication technologies such as mobile phones. The balance between educating pupils to take a responsible approach and the use of regulation and technical solutions must be judged carefully. There are a number of technical solutions to help limit internet access, although it is the appropriateness and consistency of the school's E-Safety Policy that is of overriding importance.

Regulation

The use of a finite and expensive resource which brings with it the possibility of misuse, requires regulation. In some cases, access within schools must simply be denied. For instance, un-moderated chat rooms present immediate dangers and are usually banned. Fair rules, clarified by discussion and prominently displayed at the point of access will help pupils make responsible decisions. Nova Primary School is protected by Bristol City Council's internet filter which prevents access to social networking sites.

Appropriate Strategies

This document describes strategies to help ensure responsible and safe use. They are based on limiting access, developing responsibility and guiding pupils towards educational activities. Strategies must be selected to suit the school situation and their effectiveness monitored. **There are no straightforward or totally effective solutions so staff, parents and the pupils themselves must remain vigilant.**

2. Use of the Internet

The purpose of internet use in school is to raise educational standards, promote pupil achievement and wellbeing. It also supports the professional work of staff and to enhance the school's

management information and business administration systems. Knowledge of how to apply and operate safely on the internet is vital to prepare our pupils for their future journey.

Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils to develop pupils' competence in computing skills and their general research skills.

Internet access is an entitlement for students who show a responsible and mature approach to its use.

The internet is an essential element in 21st century life for education, business and social interaction. The school therefore has a duty to provide students with quality internet access as part of their learning experience.

3. Enhancing Learning Through The Internet

To ensure that pupils are in a safe environment for learning through the internet, the following guidelines and principles should be adhered to at all times:

- The school internet access will be designed expressly for educational use and will include filtering appropriate to the age of pupils.
- Pupils will learn appropriate internet use and be given clear objectives for internet use.
- Pupils will be given clear e-safety guidelines that will be taught at least four times a year. This guidance is in accordance with up to date online resources. E-safety teaching takes place at the beginning of each academic year and then at differing points throughout the year.
- Staff should guide pupils in online activities that will support the learning outcomes planned for the pupil's age and maturity.
- Pupils will be properly trained and taught for how search safely online using relevant search engines.
- Filtering is already in effect though children should learn how to be vigilant and wary of search results including advertisments, hoax websites and irrelavent harmful information.
- Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.

ICT and e-safety together are pervasive in our curriculum.

4. Authorised Access to the Internet

- The school will keep a record of all staff and pupils who are granted internet access. The record will be kept up-to-date; for instance, a member of staff may leave or a pupil's access be withdrawn.
- Appendix 1 outlines pupils' acceptable and responsible use of the Internet.
- Appendix 2 outlines staff acceptable and responsible use of the Internet.
- Consent for use of still, video and electronic photography for web publication including Twitter is gained via the Still, Video and Electronic Photography consent form.
- In Key Stage 1, access to the internet will be by adult demonstration with directly supervised access to specific and approved online materials.
- In both Key Stages, access to the internet should be regulated and supervised by a **class teacher** and not by an external staff member such as a supply teacher.
- Parents will be informed that pupils will be provided with supervised internet access via the Pupil Information Form where reference is made to the E-Safety Policy.

5. Filtering

- The school will work in partnership with parents, Bristol City Council, DFE, TWS (Trading with Schools), CYPS (Children and Young People's Services), EditConceptsUK (edIT) and the SWGfL to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the internet Service Provider (SWGfL) via the school Computing Lead and then onto our Technician from edIT.
- The Computing Lead, teachers and our Technician (edIT) will ensure that regular checks are made to make sure the filtering methods selected are appropriate, effective and reasonable. These checks form both of these individual's job descriptions.
- Any material that the school believes is illegal must be referred to Bristol City Council's ICT helpdesk or, if applicable, the police.

6. Assessing Risks and Monitoring

- In common with other media such as magazines, books and video, some material available via the internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither Nova Primary School nor Bristol County Council can accept liability for the material accessed, or any consequences of internet access.
- A Teacher, Teaching Assistant or Learning Support Assistant will monitor pupils with SEN, when online. All staff will be informed that pupils with SEN are at greater risk online and that incidents in and outside of school should be reported as appropriate and to the designated child protection officers in school.
- The Safety Button named 'Hector' (a swimming dolphin) will be replaced with children pressing 'windows button + d' and promoting the message 'if you don't like what you see, press windows button plus d'. The 'home' button on an iPad does the same thing and should be taught to children as a way of covering something inappropriate.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Any issues regarding pupil safety will be logged on the Cpoms safeguarding system. The class teacher will have a discussion with both parents and child protection officers about this incident and offer advice in accordance to the law. See section 14.
- Methods to identify, assess and minimise risks will be reviewed regularly.
- The Headteacher and Computing Lead will ensure that the E-Safety policy is implemented and compliance with the policy monitored.

7. Managing Content

Pupils

- If staff or pupils discover unsuitable sites, the windows + d command should be used. The URL (address) and content must be reported to the South West Grid for Learning: 0870 9081708/ 0117 9037999 CYPS (Children and Young People's Services) or email: abuse@swgfl.org.uk. If applicable the police should also be notified.
- Schools should ensure that the use of internet derived materials by staff and pupils complies with copyright law.
- Specific lessons will be included within the ICT Scheme of Work that teaches all pupils how to read information from web resources.

- A nominated person will be responsible for permitting and denying additional websites as requested by colleagues.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using internet material in their own work. The school may employ technology to identify plagiarism.

Website

- The point of contact on the website should be the school address, email and telephone number. Staff or pupils' home information will not be published.
- Pictures of children on the server or elsewhere for use at school for presentations and sharing will be kept until the child's cohert leaves. After this they should be deleted. Website photographs that include pupils will be selected carefully. Please refer to the Photography Policy and Photographic Consent Form.
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
- Written permission from parents or carers, of permission or withdrawal will be obtained before pupils are published on the school website via the Still, Video and Electronic Photography Consent Form.
- Where audio and video are included (e.g. Podcasts and Video Blogging) the nature of the items uploaded will not include content that allows the pupils to be identified by their full name.
- The Headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The website should comply with the school's guidelines for publications.
- The copyright of all material must be held by the school, or be attributed to the owner where permission to reproduce has been obtained.

8. Online Communications and Social Networking

- At Nova Primary we believe that it is essential to teach children how to keep personal information safe when using online services. Each year group will have specific ICT lessons dedicated to e-safety at least four times per academic year. This guidance is in accordance with up to date online resources. E-safety teaching takes place at the beginning of each new academic year and then at differing points throughout the year. These practises will also be

referred to throughout the year and children will be consistently reminded of the risks and best choices to make online. E-safety is taught as an unbrealla across the curriculum to ensure that teachers respond sensitively to online communication and are aware that the platforms children are using are ever-changing.

- The school will conduct regular pupil monitoring about home use of computing. It will gauge the range of activities which pupils undertake and how safely they are using them, e.g. keeping personal information safe, experiences of cyber bullying and so on.
- The teachers, SLT and other staff will take an active role in engaging and talking to parents/carers about the use of unsuitable technology at home or another's home. Any issues regarding pupil safety will be logged in an e-safety record found on the teacher drive on the school server. See Section 14.
- Any negative mention of our school on social networking sites which is known will be addressed face to face with a meeting with the head teacher. Parent/carers will be advised to speak to a member of staff at school in future to resolve the problem rather than posting on a social network. Further advice can be sought from CEOPS and Bristol City Council.
- The use of online chat is not permitted in school, other than as part of its online learning environment.
- If a pupil is in breach of this policy then they will follow the school's behaviour procedure. The incident will be recorded on cpoms. The correct sanction will be given after consultation with all parties involved. The designated child protection officer should also be informed if a child is at risk.
- Our philosophy is not to ban children from ICT, but to ensure they make educated choices.
- As a school we will refer to 'Education for a Connected World' for skills to teach children about their online presence and the affect it could have on their day-to-day lives.

9. Mobile Technologies

- Appropriate use of mobile phones will be taught to pupils as part of their PHSE programme.
- Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed.
- The sending of abusive or inappropriate text messages is forbidden.
- Mobile phones should not be in school unless a specific reason is given by a parent/carer in the form of a letter. Children do not have access to a device during the day and are not permitted to have devices within classrooms, playgrounds or other public areas in school. Pupils will be

asked to give them to their teacher at the start of the school day where they are locked in the teacher's cupboard. The phone is then returned at the end of the day. Children are told about the rules of using devices in school by their teacher.

10. Cyber bullying

- Cyber bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)
- To help prevent cyber bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will also make sure pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.
- The school will actively discuss cyber bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber bullying with their classes and the issue will be addressed in assemblies.
- Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.
- As part of safeguarding training, all staff, governors and volunteers (where appropriate) receive training on cyber bullying, its impact and ways to support pupils.
- The school also sends information/leaflets on cyber bullying to parents so they are aware of the signs, how to report it and how they can support children who may be affected.
- In relation to a specific incident of cyber bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.
- The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

11. Vulnerable pupils

- A publication from the DFE ' Teaching online safety in schools' states that:

"Any pupil can be vulnerable online, and their vulnerability can fluctuate depending on their age, developmental stage and personal circumstance. However there are some pupils, for example looked after children and those with special educational needs, who may be more susceptible to online harm or have less support from family or friends in staying safe online"

- At Nova we refer to a report titled 'Vulnerable Children in a didgital world' (https://www.internetmatters.org/about-us/vulnerable-children-in-a-digital-world-report/) conducted by Interent matters, that highlights potential risks different groups of vulnerable pupils may face.
- The report splits the risks for vulnerable pupils into the 4cs – Contact, Content, Conduct and cyberscams
- It is important to remember that one size does not fit all and that the risks will vary depending on the pupil and their level of need.
- A risk assessment for a vulnerable pupil will be carried out if demmed neccassery by the class teacher.
- If appropriate, a more personalised internet safety curriculum will be taught to vulnerable pupils.

12. Pupils Knowledge of the E-Safety Policy

- Rules for internet access will be posted in all rooms where computers are used. This will be in the form of a poster.
- A module on responsible internet use and e-safety will be included in the curriculum covering both school and home use. This will include the necessity of keeping personal information safe, how to use mobile technologies appropriately and using online communication appropriately.
- Pupils will be informed that internet use will be monitored.
- Instruction on responsible and safe use should precede internet access.
- All pupils will be taught about e-safety through activities embedded at every stage of our Computing Curriculum.
- Reception and KS1 will follow the e-safety teaching of www.thinkyouknow.com and have posters displayed near computers of Hector (the swimming dolphin) and his friends.
- KS2 will follow the www.kidsmart.org.uk website to teach computing and safety skills. They will have 'Smart' posters displayed near computers in the classrooms or other areas.

13. Parents

- Parents' attention will be drawn to the School E-Safety Policy in newsletters, the school prospectus, Pupil Information Form and on the school's website.
- Regular information will be provided to parents about how to ensure they can work with the school to make sure this resource is used appropriately both within school and at home.
- Internet issues will be handled sensitively to inform parents without undue alarm.
- A partnership approach with parents will be encouraged. This could include demonstrations, practical sessions and suggestions for safe internet use at home.
- Advice on filtering systems and educational and leisure activities that include responsible use of the internet will be made available to parents.
- Interested parents will be referred to organisations such as PIN, Parents Online and NCH Action for Children (URLs in reference section).
- All parents will receive support information as and when available, e.g. http://www.kidsmart.org.uk/parents/ or from a magazine called 'Digital Parenting'.

14. Staff

- All staff including teachers, supply staff, classroom assistants and support staff, will be provided with the School's E-Safety Policy, and its importance explained.
- The school's consequences for internet and mobile phone/PDA/technology misuse will be clear so that all teachers are confident to apply this should the situation arise.
- All staff must accept the terms of the 'Acceptable and Responsible Internet Use' statement before using any internet resource in school.
- Discretion and professional conduct is essential.
- The monitoring of internet use is a sensitive matter. Staff that operate monitoring procedures should be supervised by senior management.
- Staff development in safe and responsible internet use and on the school's E-Safety Policy will be provided as required.
- All staff will receive regular E-Safety training.

15. Complaints

- Responsibility for handling incidents will be delegated to a member of SLT.
- Any complaint about staff misuse must be referred to the Headteacher.
- Pupils and parents will be informed of the complaints procedure via the school's website.
- Parents and pupils will need to work in partnership with staff to resolve issues.
- There may be occasions when the police must be contacted. Early contact could be made to establish the legal position and discuss strategies.
- Sanctions available include:
    - interview by Headteacher
    - informing parents or carers
    - removal of internet access for a period of time

16. E-Safety Logging Procedures

If you believe that there is a cause for concern regarding the safety of a pupil at home or school who may be using or have seen technology that is unsuitable please follow these steps:

1. Speak to the child and get the full story.
2. If it is an incident at school or home please speak with the child about their behaviour and write a note/speak to their class teacher. The class teacher must address this issue by talking to the parent/carer and discussing how we can help/advise. This concern must be logged – see below.
3. On Cpoms Login - CPOMS teachers should log any E-safety related incidents under the add incidents page.
4. Fill in the incident form with as much detail as you can so that we can begin to deal with the situation. Incidents must be sent to the safeguarding lead and any relevant staff.
5. Then finally, email the IT Lead and headteacher with details of the case and then we can begin to liaise with the correct people to deal with the issue.

We are all responsible for the safety of our children at Nova Primary and this includes a duty of care towards safely managing social media, e-safety and online communication. Even if the child is not in your class, TAKE ACTION!!!

Appendix 1 – Pupil's Acceptable and Responsible Internet Use

These rules help us to be fair to others and keep everyone safe.

- I will ask permission before using the internet.
- I will use only my class network login and password, which is secret.
- I will only open or delete my own files.
- I understand that I must not bring into school and use software or files without permission.
- The messages I send will be polite and sensible.
- I understand that I must never give my home address or phone number, or arrange to meet someone.
- If I see anything I am unhappy with or I receive messages I do not like, I will tell a teacher immediately.
- I understand that the school may check my computer files, and the internet sites I visit.
- I understand that if I deliberately break these rules, I may not be allowed to use the internet or computers.

The school may exercise its right to monitor the use of the school's computer systems. This includes access to websites, the interception of email and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system is or may be taking place. Alternatively the system is or may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound. Bristol City Council monitors all internet use and will notify the Local Authority if an illegal website is accessed.

Appendix 2 – Web Based Resources

For Schools

Internet Matters - https://www.internetmatters.org/
A website that educates parents on how to keep children safe online. Advice for different ages.

Hectors World - www.hectorsworld.com
KS1 and KS2 online activites teaching internet safety

DfES Anti-Bullying Advice - http://www.dfes.gov.uk/bullying/

Cyber Bullying - https://www.stopspeaksupport.com/?utm_source=Internet%20Matters
A whole school community issue

Internet Watch Foundation - www.iwf.org.uk
Invites users to report illegal websites

South West Grid for Learning – Safety www.swgfl.org.uk/safe
A comprehensive overview of web-based resources to support schools, parents and pupils

South West Grid for Learning – Filtering
http://www.swgfl.org.uk/services/default.asp?page=filtering

Think U Know - www.thinkuknow.co.uk/
Home Office site for pupils and parents explaining internet dangers and how to stay in control

Online search engine platform http://www.swiggle.org.uk

DFE updated guidance - https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/811796/Teaching_online_safety_in_school.pdf

A teaching framework to equip young children for digital life - https://www.gov.uk/government/publications/education-for-a-connected-world

For Parents

Internet Matters - https://www.internetmatters.org/
A website that educates parents on how to keep children safe online. Advice for different ages

Childnet International - http://www.childnet-int.org/
"Know It All" CD-ROM free to order resource for parents to help raise awareness of how to help their children stay safe online
Useful contact details

South West Grid for Learning (SWGfL) Support Team - (including the registering of inappropriate content needing to be filtered)
Telephone: **0870 9081708**
E-mail: support@swgfl.org.uk
To notify of an inappropriate website: abuse@swgfl.org.uk

Internet safety day:
https://www.saferinternet.org.uk/safer-internet-day/2018
Each year on safer internet day the school will:

- Promote a dialogue in each class room for how to use the internet and social media responsibly.
- Create competitions (such as designing a poster) to promote online safety.
- Model how to share our learning through the school's official social media channels.

Appendix 3 – Notes on the Legal Framework

The Computer Misuse Act 1990

The Computer Misuse Act 1990 makes it a criminal offence to gain access to a computer without permission. The motivation could be the technical challenge, data theft or to damage the system or data. The Rules for responsible internet use remind users of the ownership of the school computer system.

Monitoring of data on a school network could contravene Article 8 of the European Convention of Human Rights and Fundamental Freedoms, e.g. the right to respect for private and family life, which is protected by the Human Rights Act 1998. The Telecommunications (Lawful Practice) (Interception of Communications) Regulations 2000 also limit monitoring. The 2000 Regulations apply to all forms of electronic monitoring and interception irrespective of whether the material monitored is generated by private use or in the course of the school's day-to-day activities.

A school may only monitor authorised private use of a computer system if it can justify monitoring on the basis that it is lawful, necessary and in the interests of, amongst other things, the protection of health or morals or for the protection of the rights and freedoms of others. Schools should ensure that the monitoring is not out of proportion to the harm that could be done if the monitoring did not take place.

Schools could start by banning private use of a school's computer system, but then allow private use following the signing of an agreement to use the equipment under the conditions as laid out by the school. (A copy of the Council's policy is included in section 15). The rules for Responsible Internet Use, to which every user must agree, contain a paragraph that should ensure users are aware that the school is monitoring internet use.

In order to defend claims that it has breached either the 2000 Regulations or the Human Rights Act 1998, a school should devise procedures for monitoring, ensure monitoring is supervised by a senior manager and maintain a log of that monitoring. For example, each school can review the websites visited by the school each day/week/month. Though this is not user specific, it does allow a degree of monitoring to be conducted. All schools are also able to monitor school email.

Cyberstalking & Harassment

http://wiredsafety.org/gb/stalking/index.html)

Under Section 1 of the Malicious Communications Act 1998, it is an offence to send an indecent, offensive or threatening letter, electronic communication or other article to another person. Under Section 43 of the Telecommunications Act 1984 it is a similar offence to send a telephone message which is indecent, offensive or threatening. In both cases the offence is punishable with up to six months' imprisonment and/or a fine of up to £5,000. As the Malicious Communications Offence is more wide-ranging than the telecommunications offence it is more likely to be used by the Police than the Telecommunications Act offence.

In most cases involving malicious communications or cyberstalking however, there will be more than one offensive or threatening letter or telephone call. Therefore the police will often choose to charge the offender with an offence contrary to Section 2 of the Protection from Harassment Act 1997; also punishable with up to six months' imprisonment. Part of the reason for using this charge is that when someone is convicted of an offence under the Protection from Harassment Act 1997 the court can make a restraining order preventing them from contacting their victim again. Breach of a restraining order is punishable with up to five years' imprisonment. A restraining order cannot be imposed for a conviction under the Malicious Communications or Telecommunications Acts.

If the emails, cyberstalking etc. causes the victim to fear that violence will be used against them then the police can choose to charge the offender with an offence contrary to Section 4 of the Protection from Harassment Act 1997. This is punishable with up to five years' imprisonment and also allows the court to make a restraining order.

If the emails, cyberstalking etc. are racist in nature or motivated by religious hostility then charges could be brought of Racially or Religiously-Aggravated Harassment contrary to Sections 32(1)(a) or 32(1)(b) of the Crime and Disorder Act 1998. If convicted, offenders could face up to 7 years' imprisonment.

The fact that an offensive telephone call, letter email etc. may be received in the course of work and have been sent by a work colleague or manager does not justify the message or prevent it being an offence. Offensive messages sent within the workplace can still constitute criminal offences. In

addition they may justify a claim for constructive dismissal and compensation under employment law.

In many situations the recipient of malicious messages knows who the sender is. It may be a former partner or a relative which may mean that the victim is reluctant to involve the police. In these circumstances the victim could consider taking out an Injunction under Section 3 of the Protection from Harassment Act 1997. However we would always advise informing the police especially if the messages are in any way threatening. Even if the police decide not to prosecute they may give the offender a formal warning which could be used in evidence if they repeated their behaviour in future.

In addition to criminal prosecutions, victims of harassment can sue the offender under Section 3 of the Protection from Harassment Act 1997 for damages arising out of the anxiety caused by the harassment and any financial loss it caused.

Appendix 4 – Glossary of Terms

Blog – Short for Web Log, an online diary

DCSF - Department for Children, Schools and Families

Podcast – A downloadable sound-recording that can be played on computers and MP3 players

SWGfL – South West Grid for Learning, which provides internet access and associated managed services to all schools in the South West

Social Networking – websites that allow people to have "pages" that allow them to share pictures, video and sound and information about themselves with online friends

Video Blogging – online videos that can be uploaded via a web cam

Web 2 Technologies – a collection of online web services that are based around communicating/sharing information