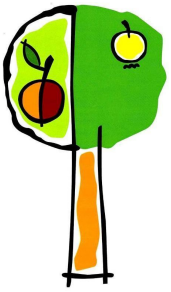
SEFTON PARK INFANTS & JUNIOR SCHOOLS



E-Safety Policy and Guidance

(Adapted BCC Policy)

Date policy adopted by Sefton Park: May 2022

Date of review: September 2023

Senior staff member responsible: Dan Simson

Next Review due: September 2023

CONTENTS

1. Core Principles of internet Safety

The internet is 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 of pupils in embarrassing, inappropriate and even dangerous situations. Schools need a policy to help to ensure responsible usage and the safety of pupils.

This E-Safety Policy is built on the following five core principles:

1.1: Guided educational use

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.

1.2: Risk assessment

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 – to become 'digitally aware'. Schools need to ensure that they are fully aware of the risks, perform risk assessments and implement a policy for internet use. Pupils need to know how to cope if they come across inappropriate material and inappropriate situations on-line. .

1.3: Responsibility

Internet safety depends on everybody: 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.

1.4: Regulation

The use of a limited and expensive resource, which brings with it the possibility of misuse, requires regulation. Fair rules, clarified by discussion and prominently displayed at the point of access will help pupils make responsible decisions.

1.5: Appropriate strategies

This document describes strategies to help to ensure responsible and safe use. They are based on limiting access, developing responsibility and on guiding pupils towards educational activities.

2. Responsibility for the Policy

Our e-safety policy has been written by the school, building on the Bristol e-safety template policy and government guidance. It has been agreed by the senior management and approved by governors. It will be reviewed annually by the senior staff member responsible for the policy.

3. Why is internet use important?

- The purpose of internet use in school is to raise educational standards, to promote pupil achievement, wellbeing and to support the professional work of staff and to enhance the school's management information and business administration systems.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
- The internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality internet access as part of their learning experience.

4. How will internet use enhance learning?

4. The school internet access will be designed expressly for educational use and will include filtering appropriate to the age of pupils.
5. Pupils will learn appropriate internet use and be given clear objectives for internet use.

- Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.

5. How will internet access be authorised?

- All staff and pupils are granted internet access. A record of staff and pupil access will be kept up-to-date; for instance a member of staff may leave or a pupil's access be withdrawn.
- Students will be required to sign an acceptable use agreement at the start of Key Stage 2 as they may well have their own school email accounts.

6. How will filtering be managed?

Levels of access and supervision will vary according to the pupil's age and experience. Internet access must be appropriate for all members of the school community from youngest pupil to staff.

The school and local authority filter internet access by cross-referencing all website requests against a banned list which is continually updated. In addition to this schools can permit or deny sites that they feel appropriate for the duration they choose.

- The school will work in partnership with parents, Bristol County Council, and Dfe ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover unsuitable sites, the URL (address) and content will be reported to the internet Service Provider 0117 9037999 cyps.it.helpdesk@bristol.gov.uk
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable. If problems are encountered with internet filtering then senior staff will refer to the IT provider for advice and support.

7. How will the risks be assessed?

- 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 international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Bristol County Council can accept liability for the material accessed, or any consequences of internet access.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Methods to identify, assess and minimise risks will be reviewed regularly.
- The headteacher and E-safety leader will ensure that the internet policy is implemented and compliance with the policy monitored.

8. Managing Content

8.1 How will pupils learn to evaluate internet content?

- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the E-safety leader.
- Specific lessons will inform pupils about copyright law and aim to ensure that the use of internet derived materials by staff and by pupils complies with copyright law.
- Specific lessons will be included within the Computing Scheme of Work that teaches all pupils how to read for information from web resources.
- A nominated person (E-safety leader or headteacher) will be responsible for permitting and denying additional websites as requested by colleagues.

8.2 How should website content be managed?

- The point of contact on the website should be the school address, school e-mail and telephone number. Staff or pupils' home information will not be published.
- Website photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified, without permission.
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
- Where parents/carers express, photographs of pupils will not be published on the school website.
- Where audio and video are included (Podcasts and Video Blogging) the nature of the items uploaded will not include content that allows the pupils to be identified.
- The headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

9. Communication

9.1 Managing e-mail

- Pupils may only use approved e-mail accounts on the school system.
- It will be made clear to pupils that they must immediately tell a teacher if they receive an offensive e-mail.
- Pupils will be taught not to reveal details of themselves or others in email communication, such as address or telephone number, or arrange to meet anyone.
- Pupils should use email in an acceptable way. Sending images without consent, messages that cause distress and harassment to others are considered significant breaches of school conduct and will be dealt with according to school behaviour policy.
- The staff code of practice makes clear that the school reserves the right to monitor email communication between staff and pupils.
- E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.

9.2 On-line communications and social networking.

- At Sefton Park we recognise the essential role of safe on-line communication. Safe use of the internet and specifically social network sites will be taught as part of the curriculum and **will remain responsive to the changing nature of technologies and current trends of on-line behaviour.**
- Pupils will be taught about how to keep personal information safe when using online services.
- Each year group will have specific Computing lessons dedicated to e-safety and being digitally aware. **The content of these lessons can be adapted to reflect the changing nature of e-safety.**
- Pupils will be advised to use nicknames and avatars when using social networking sites as part of the e-safety programme.
- Sefton Park's Personal, Sex, Health and Relationship Education (PSHRE) curriculum covers the issue of sexting to the appropriate age groups.

9.3 Mobile technologies

Pupil mobile phones are not permitted within the school. Pupils will be asked to give them to their teacher at the start of the school day and will be returned at the end of the day.

- Appropriate use of mobile phones will be taught to pupils as part of their e-safety 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.

10. Radicalisation and Extremism

The school's safeguarding policy which is available on our website and in school, covers Radicalisation and Extremism. See pages 20-21 of that policy.

10.1 Indicators of Vulnerability to Extremism and Radicalisation

1. Radicalisation refers to the process by which a person comes to support terrorism and forms of extremism leading to terrorism.

2. Extremism is defined by the Government in the Prevent Strategy as: Vocal or active opposition to fundamental British values, including democracy, the rule of law, individual liberty and mutual respect and tolerance of different faiths and beliefs. We also include in our definition of extremism calls for the death of members of our armed forces, whether in this country or overseas.

3. Extremism is defined by the Crown Prosecution Service as: The demonstration of unacceptable behaviour by using any means or medium to express views which: Encourage, justify or glorify terrorist violence in furtherance of particular beliefs. Seek to provoke others to terrorist acts. Encourage other serious criminal activity or seek to provoke others to serious criminal acts. Foster hatred which might lead to inter-community violence in the UK.

4. There is no such thing as a "typical extremist": those who become involved in extremist actions come from a range of backgrounds and experiences, and most individuals, even those who hold radical views, do not become involved in violent extremist activity.

5. Pupils may become susceptible to radicalisation through a range of social, personal and environmental factors - it is known that violent extremists exploit vulnerabilities in individuals to drive a wedge between them and their families and communities. It is vital that school staff are able to recognise those vulnerabilities.

6. Indicators of vulnerability include:

Identity Crisis – the student / pupil is distanced from their cultural / religious heritage and experiences discomfort about their place in society.

Personal Crisis – the student / pupil may be experiencing family tensions; a sense of isolation; and low self-esteem; they may have dissociated from their existing friendship group and become involved with a new and different group of friends; they may be searching for answers to questions about identity, faith and belonging.

Personal Circumstances – migration; local community tensions; and events affecting the student / pupil's country or region of origin may contribute to a sense of grievance that is triggered by personal experience of racism or discrimination or aspects of Government policy.

Unmet Aspirations – the student / pupil may have perceptions of injustice; a feeling of failure; rejection of civic life.

Experiences of Criminality – which may include involvement with criminal groups, imprisonment, and poor resettlement / reintegration.

Special Educational Need – students / pupils may experience difficulties with social interaction, empathy with others, understanding the consequences of their actions and awareness of the motivations of others.

7. However, this list is not exhaustive, nor does it mean that all young people experiencing the above are at risk of radicalisation for the purposes of violent extremism.

8. More critical risk factors could include: Being in contact with extremist recruiters. Accessing violent extremist websites, especially those with a social networking element. Possessing or accessing violent extremist literature. Using extremist narratives and a global ideology to explain personal disadvantage. Justifying the use of violence to solve societal issues. Joining or seeking to join extremist organisations. Significant changes to appearance and / or behaviour. Experiencing a high level of social isolation resulting in issues of identity crisis and / or personal crisis.

10.2 The role of Preventing Violent Extremism for Sefton Park School lies with the named Inclusion/Designated Safeguarding lead.

11. Introducing the Policy to Pupils

- Lessons on responsible internet use and being a digitally aware citizen 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.
- All children in KS2 will sign Pupil Acceptable Use Policy before accessing school computers.
- Instruction on responsible and safe use will precede internet access.
- Pupils will be informed that internet use will be monitored.

12. Parents and E-Safety

- Parents' attention will be drawn to the School E-Safety Policy in newsletters and on the school Website.
- Information will be provided to parents about how to ensure they can work with the school to ensure this resource is used appropriately both within school and home.
- Internet issues will be handled sensitively to inform parents without undue alarm.
- A partnership approach with parents will be encouraged. This could include suggestions for safe internet use at home.

13. Staff and the E-safety Policy

- All staff including teachers, supply staff, classroom assistants and support staff, will be provided with the School Internet 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 working with children must accept and sign the terms of the 'Computing Code of Practice' statement before using any internet resource in school.
- Staff development on safe and responsible internet use and on the school internet policy will be provided as required.

14. How will complaints be handled?

- Responsibility for handling incidents will be delegated to a senior member of staff.
- Any complaint about staff misuse must be referred to the headteacher.
- Pupils and parents will be informed of the complaints procedure.
- 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

14. Appendices

APPENDIX 1

Sefton Park KS2 Pupil Acceptable Use Agreement

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

These rules will keep me safe and help me to be fair to others.

- I will keep my logins and passwords secret.
- I will only edit or delete my own files and not look at, or change, other people's files without their permission.
- I will not bring files into school without permission or upload inappropriate material to my workspace.
- I am aware that some websites and social networks have age restrictions and I must respect this.
- I will only e-mail people I know, or a responsible adult has approved.
- The messages I send, or information I upload, will always be polite and sensible.
- I will not open an attachment, or download a file, unless I know and trust the person who has sent it.
- I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless a trusted adult has given permission. I will never arrange to meet someone I have only ever previously met on the Internet, unless my parent/carer has given me permission and I take a responsible adult with me.
- If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will show a teacher / responsible adult.
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.
- When using iPads or cameras, I will not take photographs of people without their permission.
- I will not save any inappropriate images or text onto iPads or the school system.
- I will put iPads back in the trolleys respectfully: plugged in, in their cases and neatly.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be held accountable and that there are consequences for my actions as there would be in accordance with the school behaviour policy. This may include loss of access to the school network / internet and contact with parents.

_____

I have read and understand these rules and agree to them.
Print name: *Signed:*
Date:

APPENDIX 2

Parent Intro Letter to Google Docs:

Sefton Park Google Apps

Dear Parent/Guardian.

Over the past term, 3 classes in year 2,4 and 5 have been trialling a new information technology system at Sefton Park. Having seen the positive impact it can have on teaching and learning, we are giving all children in years 3,4,5 and 6 the opportunity to have their own, individual Google App's for Education account.

Google App's is an operating system that your child would log on to via the internet. They would access the unique Sefton Park user account which would enable them to use facilities such as email and word processing.

I would be extremely grateful if you could take the time to read the following information below about how using Google APP's will benefit your child's learning.

Introduction

Our pupils use technology to learn. Technology is essential to facilitate the creative problem solving, information fluency, and collaboration that we see in today's societies. While we want our pupils to be active contributors in our connected world, we also want them to be safe, legal, and responsible.

Google Docs: Google Docs provides word processing, spreadsheet, drawing, and presentation software similar to Microsoft's Office suite. However, Google's applications are completely online, allowing access from any location with Internet connectivity. Google Docs also allows pupils to collaborate with other students and teachers in real-time as well as electronically submit homework items to their teachers.

Google Apps for Sefton Park: Google Apps for Education will be used to promote collaboration and communication between our pupils and teachers. Your child will receive a Google Apps user account in the SeftonParkSchools.co.uk Google Apps for EDU domain and have access to GMail and other Google Apps for EDU.

Google Mail (GMail): Sefton Park Pupils will receive a GMail account with an email address @seftonparkschools.co.uk. Email accounts will be set up with clear controls about who children can email. We wish to make clear that e-mail accounts are owned by Sefton Park and are not private. Sefton Park has the right to access pupil information at any time should the need arise.

Security: Google does have a powerful content filter, however Sefton Park cannot guarantee that students will not be exposed to unsolicited information. We will review this regularly in keeping with our e-safety policies.

APPENDIX 3

Parent Intro Letter to Google Docs (Contd.):

Being a Digital Citizen

At Sefton Park we use information and technology in safe, legal, and responsible ways. We prioritise teaching E-safety across all Year groups and embrace the following facets of being a digital citizen. Children are explicitly taught to:

- **Respect Yourself**. pupils will select online names that are appropriate, pupils will consider the information and images that they post online.
- **Protect Yourself**. Pupils will not publish personal details, contact details or a schedule of their activities.
- **Respect Others**. Pupils will not use technologies to bully or tease other people.
- **Protect Others**. Pupils will protect others by reporting abuse and not forwarding inappropriate materials or communications.

With this in mind, we are asking all children to read and agree to the School Acceptable Use Policy. We ask that you take time to read it with them so that they are clear about the responsibilities of using school systems outside of school. If you and your child are happy with the Acceptable Use Policy, then we ask that your child signs it and gives it to their class teacher. Once this is signed, their user names and accounts will be given to them.

This is an extremely exciting opportunity at Sefton Park to share learning at school with learning at home. We hope to see children at Sefton Park using Google App's for Education to bring their passions and interests to the forefront of classroom teaching.

Many thanks for taking the time to read this information.

Below are links to useful information for parents on e-safety and how to keep your child safe on-line.

Kids Smart http://www.kidsmart.org.uk/parents/advice.aspx
A downloadable PowerPoint presentation for parents

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

APPENDIX 4

Sefton Park Staff Computing Code of Practice

Staff Policy for responsible e-mail, network and internet use for Sefton Park Schools

1. I will use all ICT equipment issued to me in an appropriate way. I will not:
- Access offensive website or download offensive material.
- Make excessive personal use of the internet or e-mail.
- Copy information from the internet that is copyright or without the owner's permission.
- Place inappropriate material onto the internet.
- Will not send e-mails that are offensive or otherwise inappropriate.
- Disregard my responsibilities for security and confidentiality.
- Knowingly download files that will adversely affect the security of the laptop and school network.
- Access the files of others or attempt to alter the computer settings.
- Update web pages etc. or use pictures or text that can identify the school, without the permission of the headteacher.
- Attempt to repair or interfere with the components, software or peripherals of any computer that is the property of Sefton Park School.

2. I will only access the system with my own name and registered password, which I will keep secret.
3. I will inform the Network Manager/School's Technician as soon as possible if I know my password is no longer secret.
4. I will always log off the system when I have finished working.
5. All email communication with pupils will be conducted through the school provided gmail accounts.
6. I understand that the school may, in line with policy, check my computer files and e-mails and may monitor the internet sites I visit.
7. My files should not, routinely, be password protected by my own passwords. Should a confidential matter warrant this, I must gain permission from the headteacher and register the passwords with the headteacher.
8. If I use removable media, I will ensure that this has been carefully checked to ensure it is free from any type of virus.
9. 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 Network Manager.
10. All joke e-mails and attachments are potentially damaging and undesirable and therefore should not be used.
11. I will report immediately to the headteacher any unpleasant material or messages sent to me.
12. I understand that a criminal offence may be committed by deliberately accessing internet sites that contain certain illegal material.
13. Use for personal financial gain, gambling, political purposes or advertising is forbidden.
14. Activity that threatens the integrity of the school ICT systems, or activity that attacks or corrupts other systems, is forbidden.
15. I understand that if I do not adhere to these rules, my network access will be suspended immediately and that other disciplinary consequences may follow.

Name.....

Signature: .....

Date: .....

15. Web-based Resources

Name	Description	Website address
For Schools		
KidSmart	SMART rules from Childnet International and Know It All for Parents	http://www.kidsmart.org.uk/
Childnet International	Guidance for parents, schools and pupils	http://www.childnet-int.org/
Becta	e-Safety Advice	http://schools.becta.org.uk/index.php?section=is
Becta / Grid Club, internet Proficiency Scheme	On-line activities for Key Stage 2 pupils to teach e-safety.	http://www.gridclub.com/teachers/t_internet_safety.html
Hectors World	KS1 and KS2 online activites teaching internet safety	www.hectorsworld.com
Kent Local Authority	Additional e-safety materials (posters, guidance etc.)	http://www.clusterweb.org.uk/kcn/e-safety_home.cfm
London Grid for Learning	Additional e-safety materials (posters, guidance etc.)	http://www.lgfl.net/lgfl/sections/safety/esafety/menu/
DfES Anti-Bullying Advice		http://www.dfes.gov.uk/bullying/
Cyber Bullying	A whole school community issue	http://www.kidscape.org.uk/assets/downloads/dcsfcyberbullyingsummary.pdf
Grid Club	Advice on gaming.	http://www.gridclub.com/teachers/t_internet_safety.html
Internet Watch Foundation	Invites users to report illegal Websites	www.iwf.org.uk
South West Grid for Learning – Safe	A comprehensive overview of web-based resources to support schools, parents and pupils	www.swgfl.org.uk/safe
South West Grid for Learning – Filtering		http://www.swgfl.org.uk/services/default.asp?page=filtering
Think U Know	Home Office site for pupils and parents explaining internet dangers and how to stay in control.	www.thinkuknow.co.uk/
Bristol County Council – WISENET		http://wisenet.Bristol.gov.uk/documents/dsweb/View/Collection-922
For Parents		
Kids Smart	A downloadable PowerPoint presentation for parents	http://www.kidsmart.org.uk/parents/advice.aspx
Childnet International	“Know It All” CD-ROM free to order resource for parents to help raise	http://www.childnet-int.org/

	awareness of how to help their children stay safe online.	

16. Useful contact details:

Bristol CYPS IT

Telephone: **0117 9037999**

E-mail: **cyps.it.helpdesk@bristol.gov.uk**

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**

17. Notes on the Legal Framework

This page must not be taken as advice on legal issues, but we feel that schools should be alerted to some of the legislation that may be relevant.

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 e-mail.

Cyber-stalking & 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 and

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 £5000.

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 cyber-stalking however there will be more than one offensive or threatening letter or telephone call and 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 e-mails, cyber-stalking 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 which is punishable with up to five years' imprisonment and also allows the court to make a restraining order.

If the e-mails, cyber-stalking etc. is 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 e-mail 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 those 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.