Wandsworth Safeguarding Children Board

# e-safety policy

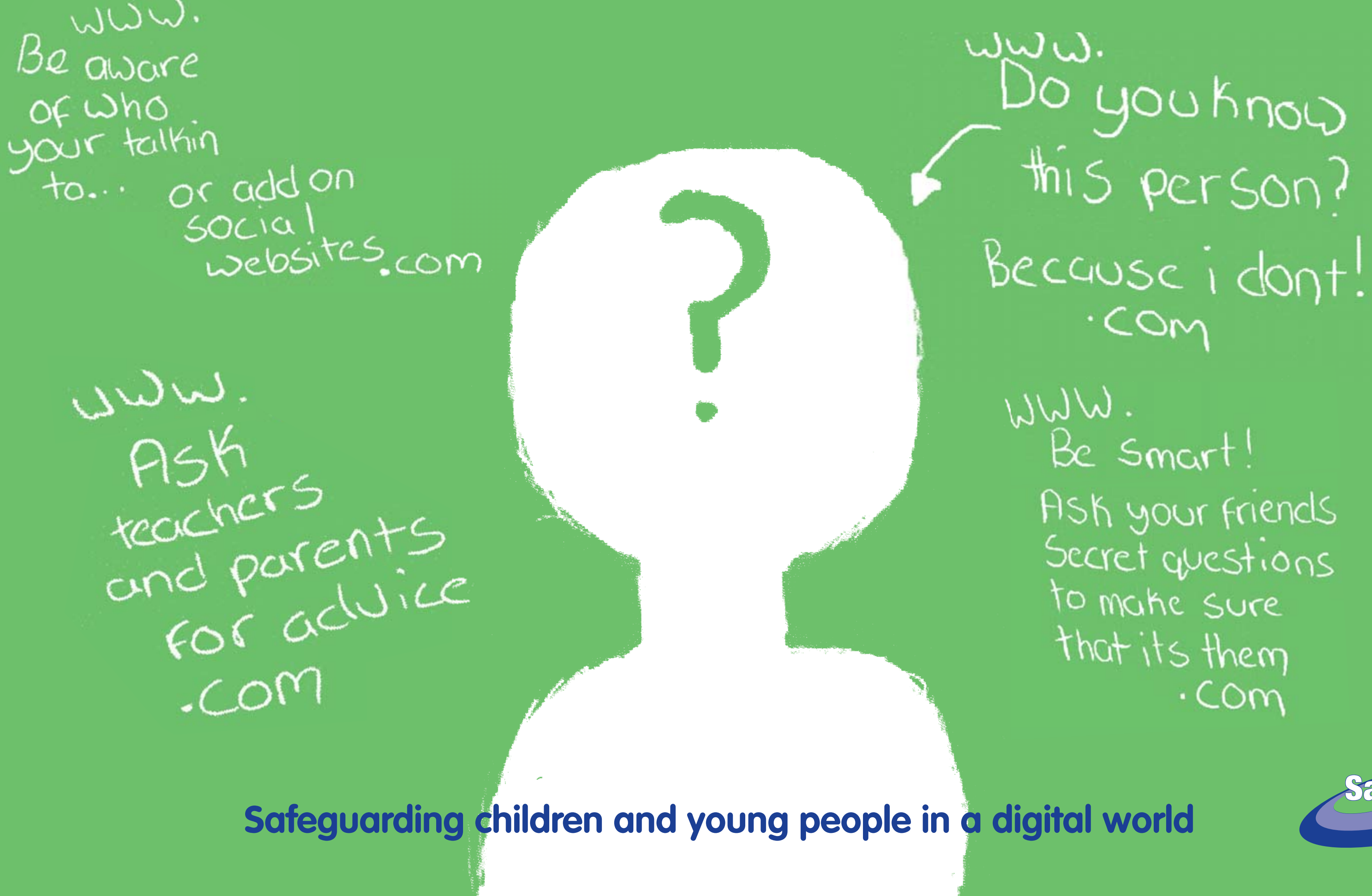

www.
Be aware of who your talkin to... or add on social websites.com
www.
Do you know this person? Because i dont!
.com
www.
Ask teachers and parents for advice
.com
www.
Be smart! Ask your friends Secret questions to make sure that its them
.com

Illustration by Adrian Thompson of South Thames College

Safeguarding children and young people in a digital world

WANDSWORTH Safeguarding CHILDREN & YOUNG PEOPLE

# Contents

*Acknowledgement: Many thanks to Kent County Council for allowing us to use their policy documentation and to London Grid for Learning for their e-safety resources.*

ICT in the 21st Century has an all-encompassing role within the lives of children and adults. Harnessing Technology: Transforming learning and children's services[1] sets out the government plans for taking a strategic approach to the future development of ICT.

***"The internet and related technologies are powerful tools, which open up new prospects for communication and collaboration. Education is embracing these new technologies as they bring with them fresh opportunities for both teachers and learners.***

***To use these technologies effectively requires an awareness of the benefits and risks, the development of new skills, and an understanding of their appropriate and effective use both in and outside of the classroom."***

*DfES, eStrategy 2005*

The Every Child Matters[2] and the provisions of the Children Act 2004[3], Working Together to Safeguard Children 2006[4] sets out how organisations and individuals should work together to safeguard and promote the welfare of children.

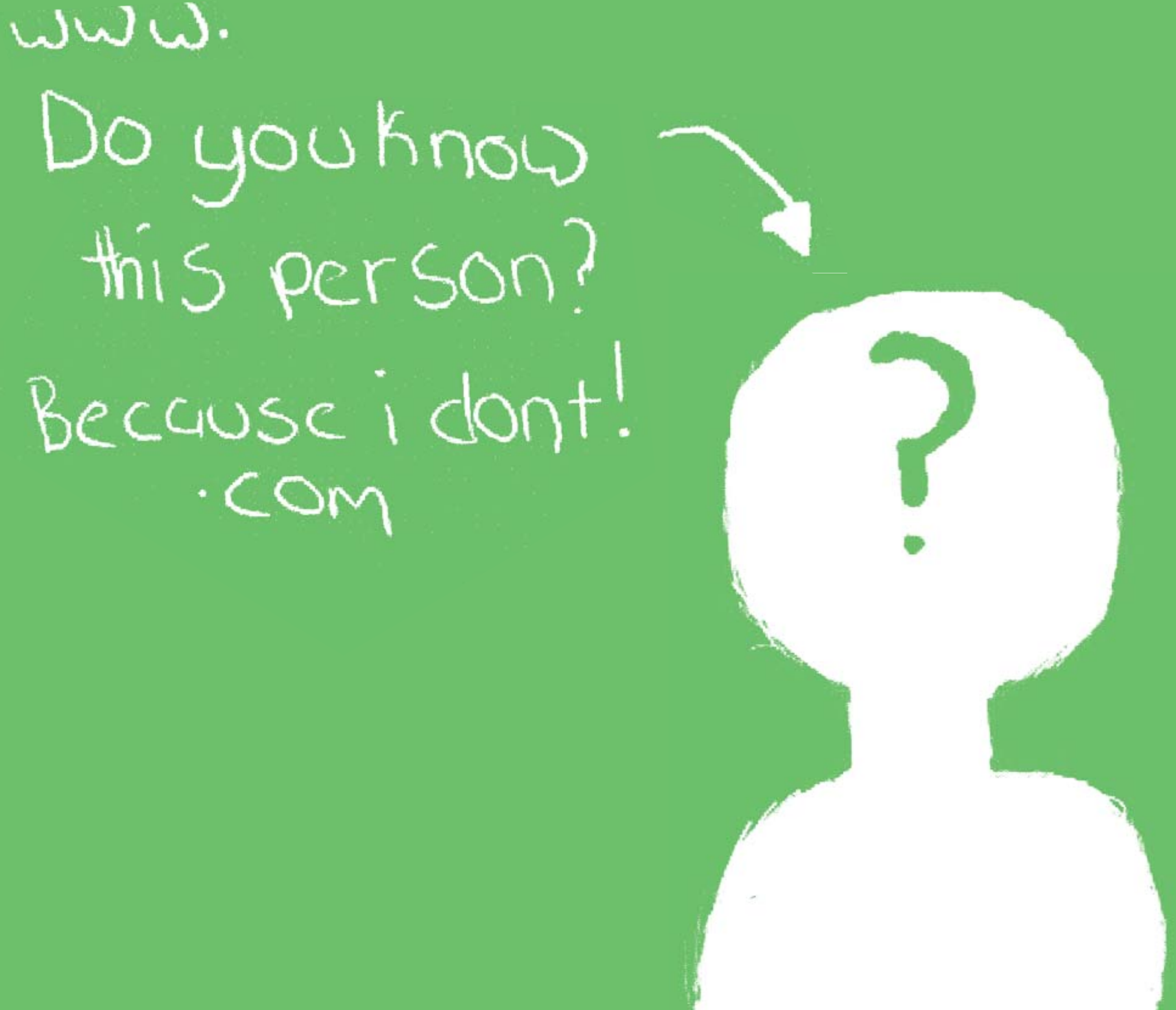
[1] www.dfes.gov.uk/publications/e-strategy

[2] See Every Child Matters website (www.everychildmatters.gov.uk)

[3] See The Children Act 2004 (www.opsi.gov.uk/acts/acts2004/20040031.htm)

[4] Full title: *Working Together to Safeguard Children: A guide to inter-agency working to safeguard and promote the welfare of children.* See Every Child Matters website (www.everychildmatters.gov.uk/_files/AE53C8F9D7AEB1B23E403514A6C1B17D.pdf)

# what is e-safety?



# What is e-safety?

e-safety encompasses not only internet technologies, but also electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits, risks and responsibilities of using information technology. It provides safeguards and raises awareness to enable users to control their online experiences.

The internet is an unmanaged, open communications channel. The world wide web, email, blogs and social networking all transmit information using the internet's communication infrastructure. Anyone can send messages, discuss ideas and publish material with little restriction. These features of the internet make it an invaluable resource used by millions of people every day.

Much of the material on the internet is published for an adult audience and some is unsuitable for children and young people. In addition, there is information on weapons, crime and racism, access to which would be more restricted elsewhere. Children and young people must also learn that publishing personal information could compromise their security and that of others.

All organisations need to protect themselves from legal challenge. The law is catching up with iInternet developments, for example it is an offence to store images showing child abuse and to use email, text or instant messaging (IM) to 'groom' children.

A new national e-safety drive is being led by the Child Exploitation and Online Protection Centre (CEOP) and detailed materials for organisations are available from the British Educational Communications and Technology Agency (Becta).

# the issues and risks

www.
Be Smart!
Ask your friends
Secret questions
to make sure
that its them
.com

# The issues and risks

As in any other area of life, children and young people are vulnerable and may expose themselves to danger - knowingly or unknowingly - when using the internet and other digital technologies.

**Examples of e-safety issues include:**

- Exposure to inappropriate material.
- Bullying via websites and mobile phones.
- The threat of danger from making contact with a criminal minority via chat rooms and social networking sites.

Research, from the **UK Children Go Online of 9-19 year olds use of the Internet between 2003-2005** concluded:

***"...the risks do not merit a moral panic, and nor do they warrant seriously restricting children's internet use because this would deny them the many benefits of the internet. Indeed there are real costs to lacking access of sufficient skills to use it. However, the risks are nonetheless widespread, they are experienced by many children as worrying or problematic, and they do warrant serious intervention by Government, educators, industry and parents."***

The aims of **Every Child Matters** outcome '**Staying Safe**' were written with the 'real' world in mind. They aim to protect children and young people from:

- maltreatment, neglect, violence and sexual exploitation
- accidental injury and death
- bullying and discrimination
- crime and anti-social behaviour in and out of school.

These aims try to ensure that children or young people have security, stability and are cared for.

However it is important to note that many of these aims have aspects, which apply even more forcefully to the 'virtual' world of the 21st Century that children and young people will encounter whenever they use ICT in its various forms. For example, we know that the internet has been used for grooming children and young people with the ultimate aim of exploiting them sexually; we know that ICT can offer new weapons for bullies, who may torment their victims via websites or text messages; and we know that children and young people have been exposed to inappropriate content when online, which can sometimes lead to their involvement in crime and anti-social behaviour.

It is the duty of all organisations to ensure that every child in their care is safe, and the same principles should apply to the 'virtual' or 'digital' world as would be applied to the physical world.

This policy document is drawn up to protect all parties - children and young people, staff and organisations and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements.

We have a moral and legal responsibility to meet the ECM agenda and to ensuring that young people become responsible e-citizens.

All partner organisations of the Wandsworth Safeguarding Children Board (WSCB) must have a co-ordinated and consistent approach to tackling e-safety so that the risks to all young people are minimised.

# The issues and risks

We also have a responsibility to ensure our workforce model good behaviours and are themselves protected.

The impact of e-safety extends to all who work with young people, especially teachers and Children's Services professionals, as communications networking can be used to negative effect against them (*"Cyber bullying is acknowledged to be driving some teachers out of the profession".* Alan Johnson, April 2007).

Organisations, have a duty of care towards all their employees. A staff member who is abused through the Internet may seek legal redress from the organisation (or borough).

**Evidence shows that:**

- LAs are often the first port of call for e-safety advice - particularly in primary education.
- While young people may be in a relatively secure environment while in school, this is not always the case at home or other locations.
- Schools have a vital role to play in fostering internet literacy (although the National Curriculum has not yet caught up with a changing world.)
- Parents often underestimate the experiences their children are exposed to.
- The risk to young people is growing, this risk changes rapidly and is likely to affect the more vulnerable.

Young people are constantly looking to 'push boundaries' and this applies to internet use in the way it would to any other area.

The key message from British Education Communications Technology Authority (Becta) is that e-safety is not an ICT issue but a whole school, and a safeguarding issue for parents, carers and all professionals.

# how we will tackle the issues

www.
Ask
parents
for advice
.com

# How we will tackle the issues

## Policies and practices

We need to develop effective policies and practices at both an WSCB and a service level to protect and inform our children and their parents to maximise the opportunities from technology and to minimise the potential negative impact of technologies.

Account should be taken of e-safety in the following policies, resources and guidance:

- Teaching and Learning.
- Anti-bullying.
- Child Protection.
- Acceptable Use of ICT.

## Infrastructure and technology

Infrastructure and technology has a key role to play in helping to protect our young people. Tools are available which can automate the process of monitoring and recording the majority of internet activity. The management of these tools must be purposeful and effective and support policy and practice.

## Education and training

All staff dealing directly with children and young people have a role to play in making sure young people are educated to become responsible e-citizens.

Professionals need to become aware of the risks facing young people and be provided with a range of strategies to enable them to teach and promote responsible use of technologies. Professionals also need to be aware of the great wealth of opportunities there are for young people using technologies to fully understand why this is so significant.

## Review and develop

Services should be encouraged to review and evaluate their provision for e-safety education.

In addition all organisations should also regularly review its policy and strategies, as well as ensure its staff are up to date with the latest developments and resources.

# the technologies

www.
Be aware
of who
you add on
social
websites.com

# The technologies

ICT in the 21st Century has an all-encompassing role within the lives of children and adults. New technologies are enhancing communication and the sharing of information.

Current and emerging technologies used by children in school and, more importantly, in many cases used outside of school include:

- **The internet**
- **Email**
- **Instant messaging** often using simple web cams, eg, www.msn.com; info.aol.co.uk/aim
- **Blogs** - an online interactive diary.
- **Podcasts** - radio or audio broadcasts downloaded to computer or MP3/4 player
- **Social networking sites** - popular sites: www.myspace.com; www.piczo.com; www.bebo.com; www.hi5.com
- **Video broadcasting sites** - a popular site is: www.youtube.com
- **Chat rooms** - popular sites: www.teenchat.com; www.habbohotel.co.uk
- **Gaming sites** - popular sites: www.neopets.com; www.miniclip.com/games/en; www.runescape.com
- **Music download sites** - popular sites: www.apple.com/itunes; www.napster.co.uk; www-kazzaa.com; www-livewire.com
- **Mobile phones** with camera and video functionality
- **Smart phones** with email, web functionality and cut down Microsoft Office applications

# the WSCB approach

www.
Ask
teachers
for advice
.com

# The WSCB approach

## WSCB wide approach to the safe use of ICT

**Creating a safe ICT learning environment in Wandsworth includes three main elements:**

- An effective range of technological tools.
- Policies and procedures, with clear roles and responsibilities.
- A comprehensive e-safety training programme for staff, children and young people and parents/carers.

## Roles and responsibilities

e-safety is recognised as an important aspect of strategic leadership in Wandsworth and the Chair of WSCB, with the support of all partner organisations and staff, aims to embed safe practices into our work. The WSCB will ensure that the e-Safety Policy is implemented and that compliance with the policy is monitored. The responsibility for e-safety has been designated to a member of the senior management team.

Wandsworth's e-Safety Co-ordinator role will be fulfilled by the e-Safety Working Group. Membership is outlined within the e-Safety Strategy or can be accessed via the website at **www.wscb.org.uk**.

Our e-Safety Coordinator ensures they keep up to date with e-safety issues and guidance through liaison with organisations such as Becta, LGfL and The Child Exploitation and Online Protection (CEOP). The e-Safety Co-ordinator ensures the WSCB, Director of Children's Services, senior management and council members are updated as necessary.

All organisations' staff that work with children are responsible for promoting and supporting safe behaviours and following e-safety procedures. Central to this is fostering a 'no blame' culture so children and young people feel able to report any bullying, abuse or inappropriate materials.

All staff should be familiar with this policy including:

- Safe use of email.
- Safe use of the internet including use of internet-based communication services, such as instant messaging and social networking.
- Safe use of network, equipment and data.
- Safe use of digital images and digital technologies, such as mobile phones and digital cameras.
- Publication of child information/photographs and use of websites.
- e-bullying/cyberbullying procedures.
- Their role in providing e-safety education for children and young people.

Staff are reminded/updated about e-safety matters at least once a year.

## How will complaints regarding e-safety be handled?

The organisations should take all reasonable precautions to ensure e-safety. However, owing to the international scale and linked nature of internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a computer or mobile device for which the organisation has responsibility. The organisation cannot accept liability for material accessed, or any consequences of internet access.

# FAQs

www.
Be aware
of who
your talkin
to .com

# FAQs

## What do we do if...

### An inappropriate website is accessed unintentionally in a school or children's setting by staff or a child.

1. Play the situation down; don't make it into a drama.
2. Report to the head/senior manager/e-safety lead officer and decide whether to inform parents of any children who viewed the site.
3. Inform the school or organisation's technical support and ensure the site is filtered (LGfL schools report to: webalerts@synetrix.com).
4. If the filtering service is provided via the LA/RBC, inform Wandsworth's e-safety officer.

### An inappropriate website is accessed intentionally by a child.

1. Refer to the acceptable use policy that was signed by the child, and apply agreed sanctions.
2. Notify the parents/carer of the child.
3. Inform the organisation's technical support and ensure the site is filtered if need be.
4. Inform Wandsworth's e-safety officer if the filtering service is provided via the LA/RBC.

### An adult uses an organisation's ICT equipment inappropriately.

1. Ensure you have a colleague with you, do not view the misuse alone.
2. Report the misuse immediately to the head/senior manager/e-safety officer and ensure that there is no further access to the PC or laptop.
3. If the material is offensive but not illegal, the head/senior manager/e-safety officer should then:
4. Remove the PC to a secure place.
5. Instigate an audit of all ICT equipment by the ICT technical support providers to ensure there is no risk of others accessing inappropriate materials.
6. Identify the precise details of the material.
7. Take appropriate disciplinary action (contact Personnel/Human Resources).
8. In an extreme case where the material is of an illegal nature:
9. Remove the PC to a secure place and document what you have done.
10. Contact the local police and follow their advice.

### A bullying incident directed at a child occurs through email or mobile phone technology.

1. Advise the child not to respond to the message.
2. Refer to relevant policies including e-safety anti-bullying and apply appropriate sanctions.
3. Secure and preserve any evidence.
4. Inform the sender's email service provider.
5. Notify parents/carers of the children involved.
6. Consider delivering a parent/carer workshop for the community.
7. Inform the police if necessary.
8. Inform Wandsworth's e-safety officer.

# FAQs

**Malicious or threatening comments are posted on an internet site about a child or member of staff.**

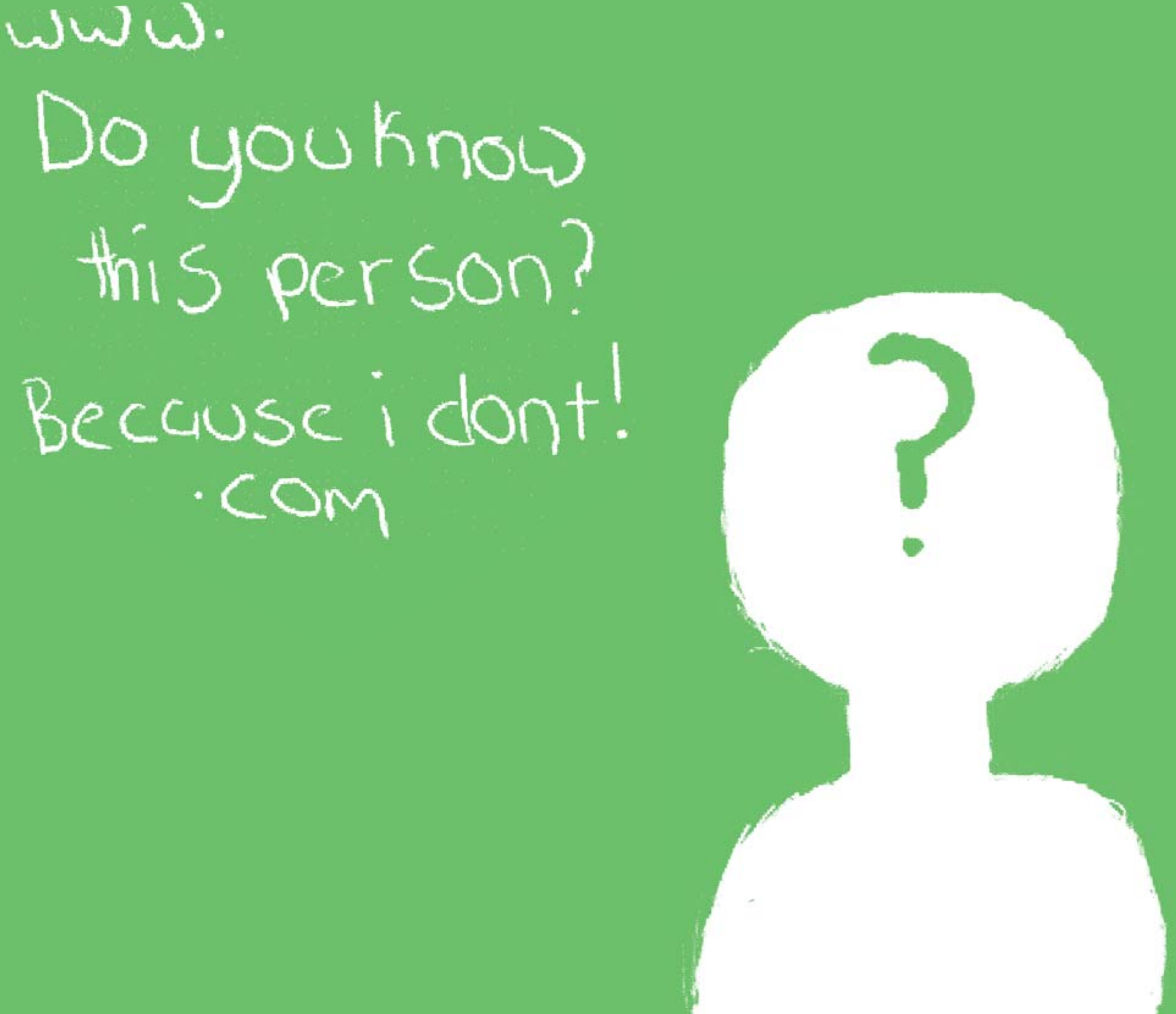
1. Inform and request the comments be removed if the site is administered externally.
2. Secure and preserve any evidence.
3. Send all the evidence to CEOP at: www.ceop.gov.uk/contact_us.html
4. Endeavour to trace the origin and inform police as appropriate.
5. Inform Wandsworth's e-safety officer.

**You are concerned that a child's safety is at risk because you suspect someone is using communication technologies (such as social networking sites) to make inappropriate contact with the child.**

1. Report to and discuss with the named child protection officer/lead officer for safeguarding and contact parents/carers.
2. Advise the child on how to terminate the communication and save all evidence.
3. Contact CEOP: www.ceop.gov.uk
4. Consider the involvement of police and Children's Services.
5. Inform Wandsworth's e-safety officer.

Children should be confident in a no-blame culture when it comes to reporting inappropriate incidents involving the internet or mobile technology - they must be able to do this without fear.

# the legal framework



# The legal framework

This section is designed to inform users of legal issues relevant to the use of electronic communications. It is not professional advice.

Many young people and indeed some staff use the internet regularly without being aware that some of the activities they take part in are potentially illegal. The law is developing rapidly and recent changes have been enacted through:

- The **Sexual Offences Act 2003**, which introduces new offences of grooming, and, in relation to making/distributing indecent images of children, raised the age of a child to 18 years old;
- The **Racial and Religious Hatred Act 2006** which creates new offences involving stirring up hatred against persons on religious grounds; and
- The **Police and Justice Act 2006** which extended the reach of the **Computer Misuse Act 1990** making denial of service attacks a criminal offence.

## Racial and Religious Hatred Act 2006

This act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material, which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

## Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence.

Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification.

It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust).

Any sexual intercourse with a child under the age of 13 commits the offence of rape.

N.B. Schools should already have a copy of **Children & Families: Safe from Sexual Crime** document as part of their child protection packs.

More information about the 2003 act can be found at **www.teachernet.gov.uk**

# The legal framework

## Communications Act 2003 (section 127)

Sending by means of the internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment.

This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

## Data Protection Act 1998

The act requires anyone who handles personal information to notify the Information Commissioner's Office of the type of processing it administers, and must comply with important data protection principles when treating personal data relating to any living individual. The act also grants individuals rights of access to their personal data, compensation and prevention of processing.

## The Computer Misuse Act 1990 (sections 1-3)

Regardless of an individual's motivation, the act makes it a criminal offence to:

- gain access to computer files or software without permission (for example using someone else's password to access files);
- gain unauthorised access, as above, in order to commit a further criminal act (such as fraud); or
- impair the operation of a computer or program (for example caused by viruses or denial of service attacks).

## Malicious Communications Act 1988 (section 1)

This legislation makes it a criminal offence to send an electronic message (email) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

## Copyright, Design and Patents Act 1988

Copyright is the right to prevent others from copying or using his or her 'work' without permission.

The material to which copyright may attach (known in the business as 'work') must be the author's own creation and the result of some skill and judgement. It comes about when an individual expresses an idea in a tangible form. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer.

It is an infringement of copyright to copy all or a substantial part of anyone's work without obtaining the author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material.

It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

## Public Order Act 1986 (sections 17-29)

This act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material, which is threatening. Like the **Racial and Religious Hatred Act 2006** it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

## Protection of Children Act 1978 (section 1)

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

## Obscene Publications Act 1959 and 1964

Publishing an 'obscene' article is a criminal offence. Publishing includes electronic transmission.

## Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.

A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

## Regulation of Investigatory Powers Act 2000

The **Regulation of Investigatory Powers Act 2000 (RIP)** regulates the interception of communications and makes it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the **Human Rights Act 1998**.

The **Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000**, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored.

Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.

# e-safety contacts & references

www.
Be smart!
Ask your friends
Secret questions
to make sure
that its them
.com

# e-safety contacts & references

**Wandsworth Children's Services**
e-Safety Officer

e esafety@wandsworth.gov.uk

**Wandsworth Children's Services**
**ICT Support**
Help with filtering and network security.

t (020) 8871 8373

**BBC Chat Guide**

w www.bbc.co.uk/chatguide

**Becta**

w www.becta.org.uk/schools/esafety

**Childline**

w www.childline.org.uk

**Child Exploitation & Online Protection Centre**

w www.ceop.gov.uk

**e-Safety in Schools**

w www.clusterweb.org.uk/esafety

**Grid Club and the Cyber Cafe**

w www.gridclub.com

**Internet Watch Foundation**

w www.iwf.org.uk

**Internet Safety Zone**

w www.internetsafetyzone.com

**Kidsmart**

w www.kidsmart.org.uk

**London Grid for Learning e-Safety resources**

w safety.lgfl.net

**NCH - The Children's Charity**

w www.nch.org.uk

**NSPCC**

w www.nspcc.org.uk/html/home/needadvice/needadvice.htm

**Stop Text Bully**

w www.stoptextbully.com

**Think U Know**

w www.thinkuknow.co.uk

**Virtual Global Taskforce - Report Abuse**

w www.virtualglobaltaskforce.com

## e-Safety Working Group:

**Clive Lett**
Inspector for Youth Engagement
Wandsworth Borough Police

c/o 112-118 Battersea Bridge Road, SW11 3AF

t (020) 8247 8201
e clive.lett@met.police.uk

**Gary Hipple**
Head of ICT and Office Services,
Wandsworth Children's Services

3rd Floor, Town Hall Extension
Wandsworth High Street, SW18 2PS

t (020) 8871 8069
e ghipple@wandsworth.gov.uk

**Alyce Esin**
Senior Education Welfare Officer
Wandsworth Children's Services

Town Hall, Wandsworth High Street, SW18 2PS

t (020) 8871 8287
e aesin@wandsworth.gov.uk

**James Stewart**
Primary Teaching & Learning Consultant (ICT)

Professional Centre, Franciscan Road, SW17 8HE

t (020) 8871 8276
e jstewart@wpct.nhs.uk

# e-safety contacts & references

**Janette Brown**
**Named Nurse, SW London &**
**St George's Mental Health Trust**

Main Building, Springfield Hospital
61 Glenburnie Road, London SW17 7SD

t (020) 8682 6391
e janette.brown@swlstg-tr.nhs.uk

**Robin Fletcher**
**Policy and Performance Officer**

Wandsworth Housing Department
17-27 Garratt Lane, London SW18 4AE

t (020) 8871 7047
e rfletcher@wandsworth.gov.uk

**John Wheeler**
**Secondary Teaching and Learning**
**Consultant (ICT)**

Professional Centre
Franciscan Road, London SW17 8HE

t (020) 8871 8750
e jwheeler@wandsworth.gov.uk

**Ileen Ashitey**
**Designated Nurse for Safeguarding Children**
**Protection and Looked After Children**

Wandsworth Primary Care Trust
St John's Therapy Centre
162 St John's Hill
London SW11 1SW

t (020) 8812 4104
e ileen.ashitey@wpct.nhs.uk

**Linde Webber**
**WSCB Development Manager**

c/o Welbeck House
43-51 Wandsworth High Street
London SW18 2PU

t (020) 8871 8610
e wscb@wscb.org.uk *or*
lwebber@wandsworth.gov.uk

# appendices

www.
Ask
teachers
for advice
.com

# Appendix A: Policy template

Wandsworth Children's Services has approved this core e-Safety Policy, which may be used by primary schools and settings as the basis to construct their own policies.

## Introduction

e-safety encompasses internet technologies and electronic communications such as mobile phones as well as collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

The previous **Internet Policy** has been revised and renamed as the **Schools' e-Safety Policy** to reflect the need to raise awareness of the safety issues associated with electronic communications as a whole.

The **Schools' e-Safety Policy** will operate in conjunction with other policies including those for student behaviour, bullying, curriculum, data protection and security.

## The core e-Safety Policy

This core e-Safety Policy provides the essential minimal school e-safety policy, and has been approved by Wandsworth Children's Services. All the elements with a W bullet are mandatory in order to protect users, the school or setting and Wandsworth Children's Services.

Optional elements, marked with an o bullet, may be added if appropriate.

## End-to-end e-safety

e-safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff, children and young people; encouraged by education and made explicit through published policies.
- Sound implementation of e-safety policy in both administration and curriculum, including secure network design and use.
- Safe and secure broadband from the London Grid for Learning including the effective management of NetSweeper filtering.
- National Education Network standards and specifications.

## Further information

**Wandsworth e-Safety Officer**
Wandsworth Children's Services ICT support

**t** (020) 8871 8373
**e** esafety@wandsworth.gov.uk
**w** www.safety.lgfl.net

# Appendix A: Policy template

## e-safety audit

This quick self-audit will help senior staff assess whether the e-safety basics are in place to support a range of activities.

| | | | |
|---|---|---|---|
| Has the school/setting an e-safety policy that complies with Wandsworth Children's Services e-safety guidance? | | | YES/NO |
| Date of latest update: | / / | The policy was agreed on: | / / |
| The policy is available for staff at: | | | |
| The policy is available for parents at: | | | |
| The Designated Child Protection Co-ordinator is: | | | |
| The e-Safety Co-ordinator is: | | | |
| Has e-safety training been provided for both students and staff? | YES/NO | Do all staff sign an ICT Code of Conduct on appointment? | YES/NO |
| Have school e-safety rules been set for students? | YES/NO | Are these rules displayed in all rooms with computers? | YES/NO |
| Do parents sign and return an agreement that their child will comply with the e-safety rules? | | | YES/NO |
| Internet access is provided by an approved educational internet service provider and complies with DCSF requirements for safe and secure access (e.g. LGfL or Wandsworth Council). | | | YES/NO |
| Has an ICT security audit has been initiated by senior staff, possibly using external expertise? | YES/NO | Is personal data collected, stored and used according to the principles of the Data Protection Act? | YES/NO |

## Schools' e-Safety Policy

The W bullets below are the essential minimum points for an e-Safety Policy.

The W elements enable demonstration that the e-Safety Policy is compliant with the Wandsworth Children's Services approved policy. Naturally, policy must be translated into practice to protect children and educate them in responsible ICT use.

### 2.1 Writing and reviewing the e-Safety Policy

The e-Safety Policy relates to other policies including those for ICT, bullying and for child protection.

W The school will appoint an e-Safety Co-ordinator. This may be the Designated Child Protection Co-ordinator as the roles overlap.

o Our e-Safety Policy has been written by the school/setting, building on Wandsworth Children's Services' e-Safety Policy and government guidance. It has been agreed by senior management and approved by governors.

o The e-Safety Policy and its implementation will be reviewed annually.

o The e-Safety Policy was revised by:

____________________________________

o It was approved by the Governors on:

____________________________________

### 2.2 Teaching and learning

### 2.2.1 Why internet use is important

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

o Internet use is a part of the statutory curriculum and a necessary tool for staff and children.

### 2.2.3 Internet use will enhance learning

W Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.

W Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

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

### 2.2.4 Children will be taught how to evaluate Internet content

W We will ensure that the use of internet derived materials by staff and children, complies with copyright law.

o Children should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

### 2.3 Managing internet access

### 2.3.1 Information system security

W ICT systems capacity and security will be reviewed regularly.

W Virus protection will be updated regularly.

W Security strategies will be discussed with Wandsworth Children's Services ICT support.

### 2.3.2 Email

W Children may only use approved email accounts on the school/setting system.

W Children must immediately tell a member of staff if they receive offensive email.

W Children must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission.

o An email sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on headed paper.

o The forwarding of chain letters is not permitted.

### 2.3.3 Published content and the school website

W The contact details on the website should be the school/setting address, email and telephone number. Staff or children's personal information will not be published.

o The head/manager will take overall editorial responsibility and ensure that content is accurate and appropriate.

### 2.3.4 Publishing children's images and work

W Photographs that include children will be selected carefully and will not enable individual children to be clearly identified.

W Children's full names will not be used anywhere on the website or blog, particularly in association with photographs.

W Written permission from parents or carers will be obtained before photographs of children are published on the school website.

o Children's work can only be published with the permission of the child and parents.

### 2.3.5 Social networking and personal publishing

W The school/setting will block/filter access to social networking sites, but may allow them for specific supervised activities.

W Newsgroups will be blocked unless a specific use is approved.

W Children will be advised never to give out personal details of any kind which may identify them or their location.

### 2.3.6 Managing filtering

W The school will work with the LA, DCSF and the internet service provider to ensure systems to protect children are reviewed and improved.

W If staff or children discover an unsuitable site, it must be reported to the e Safety Co-ordinator.

o Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

### 2.3.7 Managing video-conferencing

W IP video-conferencing should use the educational broadband network to ensure quality of service and security rather than the internet.

W Children should ask permission from the supervising member of staff before making or answering a video-conference call.

W Video-conferencing will be appropriately supervised for the children's age.

### 2.3.8 Managing emerging technologies

W Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in a school/setting is allowed.

### 2.3.9 Protecting personal data

W Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

## 2.4 Policy decisions

### 2.4.1 Authorising internet access

W All staff must read and sign the 'Acceptable ICT Use Agreement' before using any ICT resource.

W The school/setting will keep a record of all staff and children who are granted internet access. The record will be kept up-to-date, for instance a member of staff may leave or a childs access be withdrawn.

o Parents will be asked to sign and return a consent form.

### 2.4.2 Assessing risks

W The school/setting 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 computer. Neither the school/setting nor Wandsworth Council can accept liability for the material accessed, or any consequences of internet access.

W The school/setting will audit ICT provision to establish if the e-Safety Policy is adequate and that its implementation is effective.

### 2.4.3 Handling e-safety complaints

W Complaints of internet misuse will be dealt with by a senior member of staff.

W Any complaint about staff misuse must be referred to the head/senior manager.

o Complaints of a child protection nature must be dealt with in accordance with child protection procedures.

o Children and parents will be informed of the complaints procedure.

o Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

### 2.4.4 Community use of the internet

o The school/setting will liaise with local organisations to establish a common approach to e-safety.

## 2.5 Communications policy

### 2.5.1 Introducing the e-Safety Policy to children

W e-safety rules will be posted in all networked rooms and discussed with children throughout the year

W Children will be informed that network and internet use will be monitored.

### 2.5.2 Staff and the e-Safety Policy

W All staff will be given the e-Safety Policy and its importance explained.

o Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

### 2.5.3 Enlisting parents' support

W Parents/carers attention will be drawn to the e-Safety Policy in newsletters, brochures and website.

# Appendix 1: Teaching activities

## Internet use

Possible teaching and learning activities:

| Activities | Key e-safety issues | Relevant websites |
|---|---|---|
| **Creating web directories to provide easy access to suitable websites.** | Parental consent should be sought.<br>Pupils should be supervised.<br>Pupils should be directed to specific, approved online materials. | **Web directories, eg:**<br>• Ikeep bookmarks<br>• Webquest UK<br>• London Grid for Learning |
| **Using search engines to access information from a range of websites.** | Parental consent should be sought.<br>Pupils should be supervised.<br>Pupils should be taught what internet use is acceptable and what to do if they access material they are uncomfortable with. | **Web quests, eg:**<br>• Ask Jeeves for kids<br>• Yahooligans<br>• CBBC Search<br>• Kidsclick |
| **Exchanging information with other pupils and asking questions of experts via email.** | Pupils should only use approved email accounts.<br>Pupils should never give out personal information.<br>Consider using systems that provide online moderation, eg, SuperClubs. | • RM EasyMail<br>• SuperClubs PLUS<br>• Gold Star Café<br>• School Net Global<br>• Kids Safe Mail<br>• Email a children's author<br>• Email museums and galleries |

# Appendix 1: Teaching activities

| Activities | Key e-safety issues | Relevant websites |
|---|---|---|
| **Publishing pupils' work on school and other websites.** | Pupil and parental consent should be sought prior to publication. | • Making the News<br>• SuperClubs<br>• Infomapper<br>• Headline History<br>• London Grid for Learning<br>• Focus on Film |
| | Pupils' full names and other personal information should be omitted. | |
| **Publishing images including photographs of pupils.** | Parental consent for publication of photographs should be sought. | • Making the News<br>• SuperClubs<br>• Learninggrids<br>• Museum sites, etc.<br>• Digital storytelling<br>• BBC - Primary Art |
| | Photographs should not enable individual pupils to be identified. | |
| | File names should not refer to the pupil by name. | |
| **Communicating ideas within chat rooms or online forums.** | Only chat rooms dedicated to educational use and that are moderated should be used. | • SuperClubs<br>• Skype<br>• FlashMeeting |
| | Access to other social networking sites should be blocked. | |
| | Pupils should never give out personal information. | |
| **Audio and video conferencing to gather information and share pupils' work.** | Pupils should be supervised. | • Skype<br>• FlashMeeting<br>• National Archives "O-Line"<br>• Global Leap<br>• National History Museum<br>• Imperial War Museum |
| | Only sites that are secure and need to be accessed using an email address or protected password should be used. | |

If you have difficulty understanding this in English, please contact:
Wandsworth Interpreting Service: (020) 8672 1043/3649 English

যদি আপনার এটি ইংরেজিতে বুঝতে অসুবিধা হয় তাহলে অনুগ্রহ করে এখানে যোগাযোগ
করুন: Wandsworth Interpreting Service: (020) 8672 1043/3649 Bengali

Si vous avez des difficultés à comprendre ce texte en anglais, veuillez
contacter: Wandsworth Interpreting Service: (020) 8672 1043/3649 French

અગર તે અંગ્રેજીમાં સમજવી મુશ્કેલ લાગે તો મહેરબાની કરીને
Wandsworth Interpreting Service: (020) 8672 1043/3649 પર સંપર્ક કરો. Gujarati

यदि इसे अंगेजी में समझने में समस्या हो तो कृपया Wandsworth Interpreting Service
का (020) 8672 1043/3649 पर संपर्क करें। Hindi

W razie problemów ze zrozumieniem tekstu w języku angielskim prosimy
o kontakt z: Wandsworth Interpreting Service: (020) 8672 1043/3649 Polish

Se tem dificuldades em compreender isto em Inglês, por favor,
contacte: Wandsworth Interpreting Service: (020) 8672 1043/3649 Portuguese

ਜੇ ਤੁਹਾਨੂੰ, ਇਸਨੂੰ ਅੰਗ੍ਰੇਜ਼ੀ ਵਿਚ ਸਮਝਣ ਵਿਚ ਮੁਸ਼ਕਿਲ ਹੈ, ਤਾਂ ਕਿਰਪਾ ਕਰਕੇ ਸੰਪਰਕ ਕਰੋ:
Wandsworth Interpreting Service: (020) 8672 1043/3649 Punjabi

Hadday kugu adag tahay inaad ku fahamto Ingriis fadlan la xiriir:
Wandsworth Interpreting Service: (020) 8672 1043/3649 Somali

Si tiene dificultad para entenderlo en inglés favor contactar a:
Wandsworth Interpreting Service: (020) 8672 1043/3649 Spanish

இதை ஆங்கிலத்தில் புரிந்துகொளவதில் சிரமம் இருந்தால் நீங்கள் தொடர்புகொள்ள
வேண்டியது: Wandsworth Interpreting Service: (020) 8672 1043/3649 Tamil

اگر آپ کو انگریزی میں اسے سمجھنے میں دشواری کا سامنا ہو تو برائے کرم رابطہ کریں:
Urdu Wandsworth Interpreting Service: (020) 8672 1043/3649

Designed and produced by the Corporate Communications Unit, Wandsworth Council CS.366 policy (5.09)

WANDSWORTH
Safeguarding
CHILDREN &
YOUNG PEOPLE