# Downside Primary School
# ICT in Schools:
# Schools' Online Safety & ICT Policy 2020 / 21

**CONTENTS** **Page**

# 1. Aims

Our School aims to:

- Have robust processes in place to ensure the online safety of pupils, staff. volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

## 1.1 Why is Internet Use Important?

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

The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, well-being and to support the professional work of staff and to enhance the school's management information and business administration systems.

# 2. Legislation and Guidance

This policy is based on the Department for Education's statutory safeguarding guidance, 'Keeping Children Safe in Education', and its advice for schools on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department's guidance on protecting children from radicalisation.

It reflects existing legislation, including not limited to the Education Act 1996, the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' school electronic devices where they believe there is a 'good reason' to do so.

# 2. Roles and Responsibilities

## 3.1 The Governing Body

The governing body has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing body will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of school's ICT systems and the Internet (Appendix 7)

## 3.2 The Headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

## 3.3 The Designated Safeguarding Lead

Details of the school's designated safeguarding lead (DSL) are set out in our child protection and safeguarding policy.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher, ICT Lead and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged (see Appendix 10) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy

- Updating and delivering staff training on online safety (see Appendix 9)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing body

### 3.4 The ICT Manager
The ICT Manager is responsible for:
- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terroist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a monthly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

### 3.5 The ICT Lead and DSL's
The ICT Lead and DSL's are responsible for:
- Ensuring that any online safety incidents are logged (see Appendix 10) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

### 3.6 All Staff and Volunteers
All staff, including contractors and agency staff, and volunteers are responsible for:
- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the Internet (Appendix 7) and use of school's electronic devices (Appendix 6), and ensuring that pupils follow the school's terms on acceptable use (Appendix 1)
- Working with the DSL to ensure that any online safety incidents are logged (Appendix 10) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

### 3.7 Parents
Parents are expected to:
- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensuring their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and Internet (Appendices 2, 3, 4, 5)

Parents can seek further guidance on keeping children safe online from the following organisations and websites:
- What are the issues?, UK Safer Internet Centre: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues
- Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hottopics
- Parent factsheet, Childnet International: http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf

### 3.8 Visitors and Members of the Community
Visitors and members of the community who use the school's ICT systems or Internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (Appendix 7)

## 4. Educating Pupils about Online Safety

Pupils will be taught about online safety as part of the curriculum.
In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the Internet or other online technologies

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

Some of the resources we use include the 'Be Internet Legends' curriculum as well as the 'Education for a Connected World' framework as recommended in the 'Keeping Children Safe in Education 2019 Guidance'
See the schools progression framework for online safety in Appendix 11

The safe use of social media and the Internet will also be covered in other subjects where relevant. The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.
The use of online chat is not permitted in school, other than as part of its online learning environment, i.e. blogging (this is monitored at all times by the class teacher and IT Department).

## 4.1 Introducing the Policy to Pupils

Rules for Internet access will be posted in all rooms where computers are used.

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.

Instruction on responsible and safe use should precede Internet access.

Pupils will be informed that Internet use will be monitored.

All pupils will use the currently e-safety resources recommended by IT Department of LBC e.g. CEOP – Thinkuknow, to help teach internet safety.

# 5. Educating Parents about Online Safety

The school will raise parents' awareness of Internet safety in newsletters or other communications, and in information via our website. This policy will also be shared with parents.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

# 6. Cyber-bullying

## 6.1 Definition

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 inbalance of power.

## 6.2 Preventing and Addressing Cyber-bullying

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 ensure that 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. Teachers will discuss cyber-bullying with their pupils, 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, including e-safety lessons (taught once a half term). This also includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

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.

## 6.2 Examining Electronic Devices

School staff have specific power under the Education and Inspectors Act 2006 to search for and, if necessary, delete inappropriate images or files on pupils' school electronic devices, including iPads, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

Any complaints about searching for or deleting inappropriate images or files on pupils' school electronic devices will be dealt with through the school complaint procedure.

# 7. Acceptable Use of the Internet in School

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the Internet (Appendices 1 and 7). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's Internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in Appendices 1 and 7.

## 7.1 How will Internet Use Enhance Learning?

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 educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

## 7.2 How will Internet Access be Authorised?

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.
Parents will be informed that pupils will be provided with supervised Internet access (an example letter for primary schools is included as an appendix).
Primary pupils will not be issued individual email accounts, but will be authorised to us a group/class email address under supervision.
There is a structured approach to internet access and internet searches, with clear progression through the school. This can be seen in the ICT planning overview.

## 7.3 How will Filtering be Managed?

The school will work in partnership with parents, Luton Borough Council and RM Safety Net to ensure systems to protect pupils are reviewed and improved.

If staff or pupils discover unsuitable or illegal sites, the URL (address) and content must be reported to the Internet Service Provider (RM Safety Net) via the ICT Manager. Parents of the children involved will be notified immediately.

Website logs will be regularly sampled and monitored.

ICT Leader will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

# 8. Pupils using Mobile Devices in School

Pupils are not permitted to bring in any mobile device.

If a pupil is found to have a mobile device in school, teachers will inform their parents and keep the mobile device secure until it is collected by the parent/carer.

# 9. Staff using Work Devices outside School

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in Appendices 6 and 7.

Staff must ensure that their work device is secure and password-protected, and, where appropriate, encrypted, and that they do not share their passwords with others. They must take all reasonable steps to ensure the security of their work device when using it outside of school. USB devices are not permitted.

If staff have any concerns over the security of their device, they must seek advice from the ICT Manager or ICT Lead.

Work devices must be used solely for work activities.

# 10. How the School will Respond to Issues of Misuse

Where a pupil misuses the school's ICT systems or Internet, we will follow the procedures set out in the behaviour policy, The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the Internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

## 10.1 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 Luton Borough 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 ICT Leader will ensure that the Internet policy is implemented and compliance with the policy monitored.

# 11. Training

All new staff members will receive training, as part of their induction, on safe Internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation through 'Google for Education' – https://teachercenter.withgoogle.com/digital_citizenship/preview

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails and staff meetings).

Staff have also been given an Online Resilience Tool which will allow them to check if what their class is involved in online is appropriate behaviour for their age range. This can be found here https://www.headstartkernow.org.uk/Digital/Headstart%20online%20resilience%20tool%20WebV2.pdf

The DSL will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe Internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

# 12. Monitoring Arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in Appendix 10.

This policy will be reviewed every 2 years by the ICT Lead and DSL. At every review, the policy will be shared with the governing body and staff members.

## 12.1 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 ICT Manager of Luton Borough Council (Christian Turton– 01582 538200), who will the re-direct the issue to the appropriate department.

Schools should ensure that staff and pupils are aware that the use of internet derived materials should comply with current copyright laws.

Specific lessons will be included within the ICT Scheme of Work that teaches all pupils how to read for information from web resources.

Nominated persons (ICT Manager) will be responsible for permitting and denying additional websites as requested by colleagues.

## 12.2 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 identified by name.

Pupils' full names will not be used anywhere on the website, particularly in association with photographs.

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

## 12.3 Managing Email

Currently, individual pupils do not have email accounts.

Whole class email system is available, but should be activated with prior permission of the headteacher for a specific reason or project. The ICT Technician is able to activate this system with the appropriate length of notice and is monitored by the class teacher if any inappropriate issues occur.

Emails 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.

# Downside Primary School

# 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 network login and password.**
- **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, including access to web-sites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound. RM Safety Net monitors all Internet use and will notify the police and Local Authority if an illegal website is accessed.**

# Downside Primary School

## Sample Letter to Parents

### 1 September 20??

### Dear Parents

**Responsible Internet Use**

As part of your child's curriculum and the development of their ICT skills, Downside Primary School provides supervised access to the Internet. We believe that the effective use of the World Wide Web and e-mail is worthwhile and is an essential skill for children as they grow up in the modern world. All children begin the academic year learning about e-safety and follow the SMART rules to keep them safe when using the internet. These are displayed in the ICT suite to remind the children how to use the internet safely and responsibly. Please would you read the attached Rules for Responsible Internet Use and sign and return the consent form so that your child may use the Internet at school.

Although there are concerns about pupils having access to undesirable materials, we have taken positive steps to reduce this risk in school. Our school Internet provider, RM Safety Net operates a filtering system that restricts access to inappropriate materials.

Whilst every endeavour is made to ensure that suitable restrictions are placed on the ability of children to access inappropriate materials, the school cannot be held responsible for the nature or content of materials accessed through the Internet. The school will not be liable for any damages arising from your child's use of the Internet facilities.

Should you wish to discuss any aspect of Internet use please telephone the school to arrange an appointment with your child's class teacher.

Yours sincerely

## Consent Form

# Our School

## Responsible Internet Use

**Please complete, sign and return to the school secretary**

| ***Pupil:*** | ***Class:*** |
|---|---|

**Pupil's Agreement**

I have read and I understand the school Rules for Responsible Internet Use. I will use the computer system and Internet in a responsible way and follow these rules at all times.

| ***Signed:*** | ***Date:*** |
|---|---|

**Parent's Consent for Internet Access**

I have read and understood the school rules for responsible Internet use and give permission for my son / daughter to access the Internet. I understand that the school will take all reasonable precautions to ensure pupils cannot access inappropriate materials. I understand that the school cannot be held responsible for the nature or content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities.

| ***Signed:*** | ***Date:*** |
|---|---|
| ***Please print name:*** | |

**Parent's Consent for Web Publication of Work and Photographs**

I agree that, if selected, my son/daughter's work may be published on the school Website. I also agree that images, sound files and video that include my son/daughter may be published subject to the school rules and that full names will not be used.

| ***Signed:*** | ***Date:*** |
|---|---|

## Laptop policy for Downside Primary School Primary School staff (*Date*)

1. The laptop remains the property of Downside Primary School.
2. The laptop is allocated to a named member of staff and is their responsibility. If another member of staff borrows it, the responsibility still stays with the teacher allocated. Only Downside Primary School staff should use the laptop.
3. On the teacher leaving the school's employment, the laptop is returned to Downside Primary School. Staff on extended leave of 4 weeks and over should return their laptops to the school (other than by prior agreement with the headteacher).
4. When in school and not being used, the laptop must be kept in an office, locked room or drawer. It must not be left in an unlocked, unattended classroom.
5. Whenever possible, the laptop must be taken out of school and if so not be left in an unattended car. If there is a need to do so it should be locked in the boot.
6. The laptop must not be taken abroad, other than as part of a school trip and its use agreed by prior arrangement with the headteacher with evidence of adequate insurance.
7. No removable media should be used, without prior consent of the IT department/ SMT.If any removable media is used then it must be checked to ensure it is free from any viruses.
8. Staff must use their laptop in school on the network at least once a week to ensure virus protection is automatically updated and also backup their data to the designated area on the server.
9. Staff should not attempt to significantly alter the computer settings other than to personalise their desktop working area.
10. Students must never use the staff laptop.
11. If any fault occurs with the laptop, it should be referred immediately to ICT department.
12. When being transported, the carrying case supplied must be used at all times.
13. The laptop would be covered by normal household insurance. If not it should be kept in school and locked up overnight.

## Policy for responsible e-mail, network and Internet use for Downside Primary School

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.
   - Disregarded my responsibilities for security and confidentiality.
   - 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 Downside Primary 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 ICT 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. 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.

6. 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.
7. If I use removable media, I will ensure that this has been carefully checked to ensure it is free from any type of virus.
8. I will always adhere to the Downside Primary School Software Compliance Policy.
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 ICT technician.
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. Storage of e-mails and attachment should be kept to a minimum to avoid unnecessary drain on memory and capacity.
15. Activity that threatens the integrity of the school ICT systems, or activity that attacks or corrupts other systems, is forbidden.
16. I understand that if I do not adhere to these rules, my network access will be suspended immediately, my laptop removed and that other disciplinary consequences may follow.

17. I understand I cannot use any school device to access websites for personal use during school hours (including breaks / lunchtimes)

18. I will not use the school's Wi-Fi on my own personal device (s) e.g. mobile phones.

**Name……**

**Signature: ……**

**Date: ……**

# Appendix 8: Web - based Resources

## For Schools

**KidSmart** http://www.kidsmart.org.uk/
**SMART rules from Childnet International and Know It All for Parents**

**Childnet International** http://www.childnet-int.org/
**Guidance for parents, schools and pupils**

**Becta** http://schools.becta.org.uk/index.php?section=is
**e-Safety Advice**

**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

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

**Grid Club** http://www.gridclub.com/teachers/t_internet_safety.html

**Internet Watch Foundation** www.iwf.org.uk
**Invites users to report illegal Websites**
**A comprehensive overview of web-based resources to support schools, parents and pupils**

**Google 'Be Internet Legends'** https://beinternetlegends.withgoogle.com/en_uk
**Training, advice, resources for children on online safety.**

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

**Wiltshire County Council – WISENET**
http://wisenet.wiltshire.gov.uk/documents/dsweb/View/Collection-922

## For Parents

**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.**

**Internet Matters** https://www.internetmatters.org/schools-esafety/
**Lots of resources and advice on keeping children safe online.**

**Parent Zone** https://parentzone.org.uk/parents
**Lots of resources and advice on keeping children safe online.**

**Common Sense Media** https://www.commonsensemedia.org/
**Information about all types of media for children and parents.**

## Appendix 9: Online Safety Training Needs – self-audit for staff

| Online safety training needs audit | |
|---|---|
| **Name of staff member/volunteer:** | **Date:** |
| Do you know the name of the person who has lead responsibility for online safety in school? | |
| Do you know what you must do if a pupil approaches you with a concern or issue? | |
| Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors? | |
| Are you familiar with the school's acceptable use agreement for pupils and parents? | |
| Do you regularly change your password for accessing the school's ICT systems? | |
| Are you familiar with the school's approach to tackling cyber-bullying? | |
| Are there any areas of online safety in which you would like training/further training? Please record them here. | |

| | |
|---|---|
| | |

## Appendix 10: Online Safety Incident Report Log

| Online safety incident report log | | | | |
|---|---|---|---|---|
| **Date** | **Where the incident took place** | **Description of the incident** | **Action taken** | **Name and signature of staff member recording the incident** |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

# Appendix 11: Online Safety progression Framework

National Curriculum objectives

EYFS – Children recognise that a range of technology is used in places such as homes and schools. They select and use technology for particular purposes.

KS1 – Co2/1.5 – Recognise common uses of information technology beyond school.

Co2/1.6 - use technology safely and respectfully, keeping personal information private; identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

| Objective | Year R | Year 1 | Year 2 |
|---|---|---|---|
| **Self-Image and Identity** | I can recognise that I can say 'no' / 'please stop' / 'I'll tell' / 'I'll ask' to somebody who asks me to do something that makes me feel sad, embarrassed or upset.<br><br>I can explain how this could be either in real life or online. | I can recognise that there may be people online who could make me feel sad, embarrassed or upset.<br><br>If something happens that makes me feel sad, worried, uncomfortable or frightened I can give examples of when and how to speak to an adult I can trust. | I can explain that identity online and in real life might be different.<br><br>I can describe how people might make themselves look different online.<br><br>I can give examples of things that could make me feel uncomfortable and give ways I might get help. |
| **Online Relationships** | I can recognise some ways in which the internet can be used to communicate.<br><br>I can give examples of how I (might) use technology to communicate with people I know. | I can use the internet with adult support to communicate with people I know.<br><br>I can explain why it is important to be considerate and kind to people online. | I can use the internet to communicate with people I don't know well.<br><br>I can give examples of technology I may use to do this. |
| **Online Reputation** | I can identify ways that I can put information on the internet. | I can recognise that information can stay online and could be copied.<br><br>I can describe what information I should not put online without asking a trusted adult first. | I can explain that information online about me can last a long time.<br><br>I know who to talk to if I see something about me or a friend I don't like online. |
| **Online Bullying** | I can describe ways that some people can be unkind online.<br><br>I can offer examples of how this can make others feel. | I can describe how to behave online in ways that do not upset others and can give examples. | I can give examples of what bullying can look like online.<br><br>I understand how bullying can make someone feel.<br><br>I can talk about how someone would get help if they were being bullied. |
| **Managing Online Information** | I can talk about how I can use the internet to find things out. | I can use the internet to find things out.<br><br>I can use simple keywords in search engines. | I can use keywords on and navigate a simple search engine.<br><br>I can explain what a voice navigated search is and |

| | | | |
|---|---|---|---|
| | I can identify devices I could use to access information on the internet.<br><br>I can give simple examples of how to find information (e.g search engine, voice activated searching). | I can describe and demonstrate how to get help from a trusted adult or helpline if I don't like the content. | explain when it might be used (alexa, siri).<br><br>I can explain the difference between things that a true and real and explain why some information may not be true. |
| **Health, Well-being and Lifestyle** | I can identify rules that help keep us safe and healthy in and beyond the home when using technology.<br><br>I can give some examples. | I can explain rules to keep us safe when we are using technology both in and beyond the home.<br><br>I can give examples of some of these rules. | I can explain simple guidance for using technology in different environments and settings.<br><br>I can say how those rules/guides can help me. |
| **Privacy and Security** | I can identify some simple examples of my personal information (e.g name, address, birthday, age, location)<br><br>I can describe the people I can trust and share this with; I can explain why I trust them. | I can recognise my personal information.<br><br>I can explain why I must ask an adult before sharing information.<br><br>I can explain how passwords can be used to protect information. | I can explain that information about me may be seen by others.<br><br>I can explain what passwords are and can use passwords.<br><br>I can describe some rules for keeping my information private. |
| **Copyright and Ownership** | I know that work I create belongs to me.<br><br>I can name my work so that others know it belongs to me. | I can explain why work I create belongs to me.<br><br>I can save my work so others know it belongs to me. | I can describe why other people's work belongs to them.<br><br>I can recognise that content on the internet may belong to other people. |

National Curriculum Objectives

KS2 – Co2/1.4 – understand computer networks including the internet; how they can provide multiple services, such as the world wide web; and the opportunities they offer for communication and collaboration

Co2/1.5 – use search technologies effectively, appreciate how results are selected and ranked, and be discerning in evaluating digital content

Co2/1.7 – use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact.

| Objective | Year 3 | Year 4 | Year 5 | Year 6 |
|---|---|---|---|---|
| **Self-Image and Identity** | I can explain what identity means.<br><br>I can explain how I can represent myself differently online.<br><br>I can explain why I might change my identity depending on what I am doing online. | I can explain how my online identity can be different to the identity I present in 'real life'.<br><br>I can describe the right decisions about how I interact with others and how others perceive me. | I can explain how online identity can be copied, modified or altered.<br><br>I can demonstrate responsible choices about my online identity. | I know that the media can shape ideas about gender and can challenge and reject inappropriate messages.<br><br>I can describe issues that make me feel sad, worried or uncomfortable and explain why I need to keep asking until I get help. |
| **Online Relationships** | I can describe ways people can communicate online and how (emojis, text speak).<br><br>I can explain risks of communicating online and that I need to be careful who I trust.<br><br>I can explain what knowing someone online means and how to trust them. | I can describe strategies for safe and fun experiences in a range of online social environments.<br><br>I can give examples of how to be respectful to others online. | I can explain some people online may want to do me or my friends harm.<br><br>I can make positive contributions to online communities and describe this. | I understand my responsibilities for the well-being of my social group.<br><br>I can demonstrate how I would support others online and show how to block/report for myself and others. |
| **Online Reputation** | I can search for information about myself online.<br><br>I know I need to be careful before sharing anything. | I can describe how others can find out information about me by looking online.<br><br>I can explain ways that some of the information about me | I can search for information online and create a summary report.<br><br>I can describe ways that information can be | I can explain I am developing an online reputation which will allow people to form an opinion of me.<br><br>Describe simple ways that help build |

| | | | | |
|---|---|---|---|---|
| | I know who to ask before putting something online. | online could have been created, copied or shared by others. | used to make judgements. | a positive online reputation. |
| **Online Bullying** | I can explain what bullying is and can describe how people may bully others.<br><br>I can describe how to behave online and follow this. | I can identify where online bullying may take place.<br><br>I can describe ways people can be bullied (image, video, text, chat).<br><br>I can explain why I need to think carefully about what I post. | I can recognise when someone is upset online and know how to get help.<br><br>I can explain how to block or report.<br><br>I can describe helpline services who could support me. | Describe how to capture bullying content as evidence (screen shot, URL, profile) so I can get help.<br><br>Identify ways to report at school and at home. |
| **Managing Online Information** | I can explain what autocomplete is.<br><br>I can explain how the internet is used to buy and sell things.<br><br>I can explain the difference between a 'belief, opinion and fact'. | I can analyse what is an opinion, a belief or a fact.<br><br>I know that because lots of people share a belief online, it doesn't make it true.<br><br>I can describe some methods used to persuade people to buy things online (advertising, in-app purchases, pop-ups).<br><br>I know that some people online could be pretending to be someone else. | I understand the vocabulary – data, information, true, false, valid, and reliable and evidence.<br><br>I understand the difference between mis-information and dis-information.<br><br>I can explain why some information online may not be true or accurate. | I can use search technologies effectively, know how they are used and apply strategies to be discerning in evaluating digital content.<br><br>I can describe how some online information can be opinion but people may present it as facts.<br><br>I can demonstrate strategies to analyse and evaluate validity of facts and explain why the strategies are important. |
| **Health, Well-being and Lifestyle** | I can explain why spending too much time online can be bad for me.<br><br>I can give examples of activities where it is easy to spend a lot of time engaged (games, films, videos) | I know that technology can distract me.<br><br>I can identify times when I need to limit my screen time.<br><br>I can suggest strategies to help me limit this time. | I can describe ways technology can affect healthy sleep.<br><br>I can describe strategies, tips or advice to promote healthy sleep. | I can describe common systems that regulate age-related content (PEGI, BBFC, parental warnings) and describe their purpose.<br><br>I can assess and action different strategies to limit the impact on my health and explain the importance of self-regulating my time on technology. |

| | | | | |
|---|---|---|---|---|
| **Privacy and Security** | Give reasons why I should only share information with someone I trust.<br><br>I understand why passwords are important.<br><br>I can describe simple strategies for keeping passwords private.<br><br>I can describe how connected devices can share my information with others. | I know what a strong password is.<br><br>I can describe ways to keep personal information private.<br><br>I know that others may pretend to be me online and know how.<br><br>I can explain how internet use can be monitored. | I can create a strong password.<br><br>I can explain how many free apps or services share my information with others.<br><br>I can explain why some apps may take payment for additional content and why I should seek permission. | Use different passwords, know how to manage them and know what to do if I lose them.<br><br>I can explain what app permission are and give some examples.<br><br>I can describe ways to increase privacy. |
| **Copyright and Ownership** | I can explain why copying someone else's work from the internet without permission can cause problems.<br><br>I can give example of the problems. | When searching the internet for content to use I can explain why I need to consider who owns it and if I have the right to reuse it. | I can assess and justify when it is acceptable to use the work of others.<br><br>I can give examples of content that is permitted to be reused. | Demonstrate the use of search tools to find and access online content which can be used by others.<br><br>Demonstrate how to make references to and acknowledge sources I have used from the internet. |

# 14. 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.

# 15. Glossary of Terms

Blog – Short for Web Log, an online diary

DCSF - Department for Children, Schools and Families

DSL – Designated Safeguarding Lead

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

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