DOROTHY STRINGER SCHOOL

EDUCATION FOR LIFE

Cyber Security Policy

Last reviewed: March 2026

Next review due: Spring 2029

www.dorothy-stringer.co.uk

Contents

Introduction

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school.

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and Students learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to internet access within school that is safe at all times.

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. A school e-safety policy should help to ensure safe and appropriate use. The development and implementation of such a strategy should involve all the stakeholders in a child's education from the headteacher and governors to the senior leaders and classroom teachers, support staff, parents, members of the community and the Students themselves.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote student / student achievement.

However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is used in conjunction with other school policies (eg behaviour, anti-bullying and child protection policies).

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build students' / students' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

Scope of the Policy

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

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

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

Policy Statements

Education – Students

Whilst regulation and technical solutions are very important, their use must be balanced by educating Students to take a responsible approach. The education of Students in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience. E-Safety education will be provided in the following ways: (depending on the age of the students)

- A planned e-safety programme should be provided as part of ICT / PHSE / other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school
- Key e-safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- Students should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information
- Students should be helped to understand the need for the student AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Staff should act as good role models in their use of ICT, the internet and mobile devices

Education – parents / carers

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the

internet and are often unsure about what they would do about it. “There is a generational digital divide”. (Byron Report).

The school will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters, web site, SLG
- Parents evenings
- Reference *to external sites such as CEOPs*

Education & Training – Staff

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal e-safety training will be made available to staff. An audit of the e-safety training needs of all staff will be carried out regularly. *It is expected that some staff will identify e-safety as a training need within the performance management process.*
- **All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policies**
- *The E-Safety Coordinator (or other nominated person) will receive regular updates through attendance at / LA / other information / training sessions and by reviewing guidance documents released by BECTA / LA and others.*
- *The E-Safety Coordinator (or other nominated person) will provide advice / guidance / training as required to individuals as required*

Technical – infrastructure / equipment, filtering and monitoring

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

- **School ICT systems will be managed in ways that ensure that the school meets e-safety technical requirements**
- **There will be regular reviews and audits of the safety and security of school ICT systems by the Network Manager, which will be presented to SLT**
- **Servers, wireless systems and cabling must be securely located and physical access restricted**

- **All users will have clearly defined access rights to school ICT systems.** *Details of the access rights available to groups of users will be recorded by the Network Manager (or other person) and will be reviewed, at least annually*
- **All users will be provided with a username and password** by *who will keep an up to date record of users and their usernames. Users will be required to change their password every year.*
- **The “master / administrator” passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the Headteacher or other nominated senior leader and kept in a secure place (e.g., school safe)**

- (Alternatively the Headteacher, other nominated senior leader or Network Manager should be allocated those master / administrator rights. A school should never allow one user to have sole administrator access)
- *Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.*
- *Users' accounts will be deleted when a user ceases employment with the school. Any data will be deleted and the associated email account will be inactive.*
- *The school maintains and supports a managed filtering service*
- *In the event of the Network Manager (or other person) needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher (or other nominated senior leader).*
- *Requests from staff for sites to be removed from the filtered list will be considered by the Network Manager and Richard Baker. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly*
- *School ICT technical staff regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Policy.*
- *The Network Manager must ensure that appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.*
- *No executable files may be downloaded by users*
- *An agreed policy is in place regarding the extent of personal use that users (staff /* Students */ community users) and their family members are allowed on laptops and other portable devices that may be used out of school.*
- *Staff are not allowed to install programmes on school workstations / portable devices.*
- *The use of memory sticks and removable devices is described in the AUP*
- *The school infrastructure and individual workstations are protected by up to date virus software.*
- *Personal data can not be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.* [Accessing such information on the SLG is considered a secure connection] (see Data Safety in the appendix for further detail)

Data Backup and Recovery

The school maintains a robust backup strategy to ensure the availability and integrity of educational and administrative data.

- **Automated Scheduling:** Core systems, including student information (SIMS), child protection records (CPOMS), and financial data, are backed up automatically on a regular schedule.
- **Off-site and Offline Storage:** To protect against physical disasters like fire or flood, as well as network-wide ransomware, backups are stored securely off-site and include "air-gapped" or immutable copies that are not permanently connected to the live network.

- **Integrity Testing:** The Network Manager is responsible for periodically testing backups to ensure that data can be fully restored in the event of system malfunctions or cyber-attacks.
- **Staff Responsibility:** While central systems are backed up by the IT team, staff are responsible for ensuring that all professional documents are saved to the school network or approved cloud storage (e.g., OneDrive) rather than solely on local device hard drives.
- **Encryption:** All backup media containing personal or sensitive data must be encrypted to prevent unauthorized access if the physical media is lost or stolen.

Curriculum

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

- *In lessons where internet use is pre-planned, it is best practice that* students *should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.*

  Similar precautions and practice should also apply to homework which is directed to the internet
- *Where* students *are allowed to freely search the internet, eg using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.*
- *Where* students *are asked to research the internet (for home especially), guidance should be given to keep them on safe sites, and also so that they do not get 'lost' (spending large amounts of time looking for something).*
- *It is accepted that from time to time, for good educational reasons,* students *may need to research topics (eg racism, drugs, discrimination, etc) that would normally result in internet searches being blocked. In such a situation, staff can request that the Network Manager (and other relevant person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.*
- Students *should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information*
- Students *should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.*

Use of digital and video images - Photographic, Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff and students need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- **When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g., on social networking sites.**
- *Staff are allowed to take digital / video images to support educational aims, but are responsible for any data. They must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.*
- *Care should be taken when taking digital / video images that* students *are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.*
- Students *must not take, use, share, publish or distribute images of others without their permission*
- *Photographs published on the website, or elsewhere that include* students *will be selected carefully and will comply with good practice guidance on the use of such images.*
- Students*' full names will not be used anywhere on a website or blog, particularly in association with photographs.*
- *Written permission from parents or carers will be obtained before photographs of* students *are published on the school website (this is covered by the parental consent which each parent signs)*

Data Protection & GDPR

Personal data will be recorded, processed, transferred and made available according to the GDPR which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

Staff must ensure that they:

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

When personal data is stored on any portable computer system, USB stick or any other removable media:

- the data must be encrypted and password protected
- the device must be password protected (many memory sticks / cards and other mobile devices cannot be password protected)
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

Please see the Data Protection Policy for more details

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. When using communication technologies, the school considers the following as good practice:

- **The official school email service may be regarded as safe and secure and is monitored.** *Staff and* students *should therefore use only the school email service to communicate with others when in school, or on school systems (e.g., by remote access).*
- **Users need to be aware that email communications may be monitored**
- **Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.**
- **Any digital communication between staff and students or parents / carers (email, chat, VLE etc) must be professional in tone and content.** *These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications.*
- Students *should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.*

Responding to Incidents of misuse

Any reports should be passed on to Richard Baker who will consider the appropriate course of action. Breaches of this policy will be dealt with at a level appropriate to the seriousness of the

alleged misconduct. Sanctions may include suspension/removal of Internet access, suspension/removal of network account and/or any normal school sanctions. Where necessary, external agencies may be involved.

- Staff procedure if students have inappropriate material on their mobiles
- *Reporting incidents of lost information*

School Filtering Policy

The school connects to the internet via the Local Authority. They filter the content before the school's systems. The school has filtering software and has responsibility for those areas which it has requested the Authority to unblocked.

Sites can be requested to be unblocked from the Authority only by the Network Manager with the Senior member of staff. If a member of staff wishes a site to be unblocked, they should submit the request and the reasons for this to the Network Manager. This will need to be approved by him and the Senior member of staff and then the request passed on if appropriate. If the site is one which the school's filtering controls, then the Senior member of staff and the Network manager must agree before any site is opened up.

Appendices

Can be found on the following pages:

Student / Student Acceptable Usage Policy

W:\Staff Shared Work\Staff Info\School Documents\Policies\AUP for DSS 09-10.doc

Staff and Volunteers Acceptable Usage Policy

W:\Staff Shared Work\Staff Info\School Documents\Policies\AUP Staff 2012.docx

School Password Policy

W:\Staff Shared Work\Staff Info\School Documents\Policies\password_policy.docx

Data Safety

W:\Staff Shared Work\Staff Info\School Documents\Policies\Data Protection Policy.doc

Responsibility of using the school systems

W:\Staff Shared Work\Staff Info\School Documents\Policies\Internet Use Statement 2012.docx

Cyber Bullying

W:\Staff Shared Work\Staff Info\School Documents\Policies\Cyber bullying Policy - draft.doc

Using Mobile Devices

W:\Staff Shared Work\Staff Info\School Documents\Policies\Use of Portable Devices.docx

Social Media

General - W:\Staff Shared Work\Staff Info\School Documents\Policies\Social networking 2012.docx

Streaming Media

W:\Staff Shared Work\Staff Info\School Documents\Policies\Streaming Media Guidelines.docx

Email Policy - W:\Staff Shared Work\Staff Info\School Documents\Policies\Dorothy Stringer Email Policy 07 - draft.doc

Email Etiquette **- The document can be viewed at** W:\Staff Shared Work\Staff Info\School Documents\Policies\Email etiquette 07.doc

Glossary of terms

Legislation

Schools should be aware of the legislative framework under which this E-Safety Policy template and guidance has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

It is recommended that legal advice is sought in the advent of an e safety issue or situation.

Computer Misuse Act 1990

This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- "Eavesdrop" on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

GDPR 2018

This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully.

Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications Act 2003

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.

Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;

- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
- Ascertain whether the communication is business or personal;
- Protect or support help line staff.
- The school reserves the right to monitor its systems and communications in line with its rights under this act.

Copyright, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. youtube).

Telecommunications Act 1984

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they: -

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

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.

Protection from Harrassment 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.

Protection of Children Act 1978

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 a 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.

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.

Public Order Act 1986

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. Children, Families and Education Directorate page 38 April 2007.

Obscene Publications Act 1959 and 1964

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

Human Rights Act 1998

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of “higher law”, affecting all other laws. In the school context, human rights to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

The Education and Inspections Act 2006

Empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

Appendix: Cyber Security Incident Management Plan

1. Immediate Response & Triage

In the event of a suspected cyber attack or data breach, staff must act immediately to contain the threat.

- **Reporting:** Any security breaches, phishing attempts, loss of equipment, or suspected misuse of ICT must be reported immediately to the Headteacher (Matt Hillier) and the Data Protection Officer (Richard Baker).
- **Containment:** If a device is suspected of being infected with malware or ransomware, it should be isolated from the network (e.g., by disabling Wi-Fi or unplugging ethernet) but not necessarily powered off, as this may erase volatile evidence.
- **Initial Assessment:** Network support will investigate to determine if the breach is an unintentional small-scale incident or an intentional large-scale attack.

2. Core Response Phases

The school follows a structured "Core Response" workflow to manage and remediate incidents:

- **Analysis:** Network support will capture and analyze data to identify the source of the attack, such as phishing, malware, or a zero-day exploit.
- **Remediation/Eradication:** The IT team will fully remove or stop the incident, which may involve running school-wide antivirus scans, patching vulnerabilities, or forcing password resets.
- **Recovery:** Systems and data will be restored from secure backups to resume "business as usual" once remediation is confirmed successful.

The 2026 Legal Position on Payments

- **Public Sector Ban**: As of 2026, there is a strong government push and legal expectation that public sector organizations, including schools, **do not pay ransoms**.
- **No Guarantees**: Paying a ransom does not guarantee the data will be decrypted, does not remove the malware from your system, and makes the school a more likely target for future attacks.
- **Legal Reporting**: Any ransomware incident must be reported to the government within **72 hours**.

3. External Notification & Reporting

Depending on the severity and nature of the attack, the school is obligated to inform the following external bodies:

- **Local Police & Education Team:** For criminal activity or threats to the school community.
- **National Cyber Security Centre (NCSC):** Via the official reporting portal.
- **Action Fraud:** For any incidents involving financial fraud or scams.

- **Department for Education (DfE):** In line with statutory reporting requirements for schools.

4. Post-Incident Actions

- **Review and Close Down:** Following the resolution of an incident, the IT team will document the event and assign improvements to prevent a recurrence.
- **Password Resets:** If a device is stolen or an account is compromised, all associated account passwords must be changed immediately.
- **Disciplinary Action:** The school will examine incidents on a case-by-case basis. Intentional or repeated breaches may lead to formal disciplinary action or termination.