# Student/Pupil Acceptable Use Agreement Template – for older students/pupils

Sections that include advice or guidance are written in BLUE. It is anticipated that schools will remove these sections from their final Acceptable Use document. Schools should review and amend the contents of this agreement to ensure that it is consistent with their Online Safety Policy and other relevant school policies. Due to the number of optional statements and the advice/guidance sections included in this template, it is anticipated that the final document will be more concise. Schools will need to decide on the suitability of the statements/language used and may wish to amend these in light of the age/abilities of the students/pupils.

## School Policy

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe access to these digital technologies.

### This acceptable use agreement is intended to ensure:

* that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
* that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and will have good access to digital technologies to enhance their learning and will, in return, expect the *students/pupils* to agree to be responsible users.

## Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.

### For my own personal safety

* I understand that the *school* will monitor my use of the systems, devices and digital communications.
* I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person’s username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
* I will be aware of “stranger danger”, when I am communicating on-line.
* I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc.)
* If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
* I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

### I understand that everyone has equal rights to use technology as a resource and

* I understand that the *school* systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
* I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
* I will not use the *school* systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube), unless I have permission of a member of staff to do so. (schools should amend this section to take account of their policy on each of these issues)

25

### I will act as I expect others to act toward me

* I will respect others’ work and property and will not access, copy, remove or otherwise alter any other user’s files, without the owner’s knowledge and permission.
* I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
* I will not take or distribute images of anyone without their permission.

### I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the *school*

* I will only use my own personal devices (mobile phones/USB devices etc.) in school if I have permission (schools should amend this section in the light of their mobile devices policies). I understand that, if I do use my own devices in the *school,* I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
* I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
* I will immediately report any damage or faults involving equipment or software, however this may have happened.
* I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person/organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
* I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.
* I will only use social media sites with permission and at the times that are allowed (schools should amend this section to take account of their policy on access to social media).

### When using the internet for research or recreation, I recognise that

* I should ensure that I have permission to use the original work of others in my own work
* Where work is protected by copyright, I will not try to download copies (including music and videos)
* When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

### I understand that I am responsible for my actions, both in and out of school

* I understand that the *school* also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be online-bullying, use of images or personal information).
* I understand that if I fail to comply with this Acceptable Use Policy Agreement, I may be subject to disciplinary action. This could include (schools should amend this section to provide relevant sanctions as per their behaviour policies) loss of access to the school network/internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

**Please complete the sections on the next page to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school systems and devices.**

## Student/Pupil Acceptable Use Agreement Form

This form relates to the *student/pupil* Acceptable Use Agreement; to which it is attached.

Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school systems. (Schools will need to decide if they require students/pupils to sign, or whether they wish to simply make them aware through education programmes/awareness raising).

I have read and understand the above and agree to follow these guidelines when:

* I use the *school* systems and devices (both in and out of school)
* I use my own devices in the *school* (when allowed) e.g. mobile phones, gaming devices USB devices, cameras etc.
* I use my own equipment out of the school in a way that is related to me being a member of this *school* e.g. communicating with other members of the school, accessing school email, VLE, website etc.

Name of Student/Pupil:

Group/Class:

Signed:

Date:

Parent/Carer Countersignature (optional)

It is for schools to decide whether or not they require parents/carers to sign the Parent/Carer Acceptable Use Agreement (see template later in this document). This includes a number of other permission forms (including digital and video images/biometric permission/cloud computing permission).

Some schools may, instead, wish to add a countersignature box for parents/carers to this student/pupil Acceptable Use Agreement.

# Student/Pupil Acceptable Use Policy Agreement Template For Younger Pupils (Foundation/KS1)

#### This is how we stay safe when we use computers:

* I will ask a teacher or suitable adult if I want to use the computers/tablets
* I will only use activities that a teacher or suitable adult has told or allowed me to use
* I will take care of computers/tablets and other equipment
* I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong
* I will tell a teacher or suitable adult if I see something that upsets me on the screen
* I know that if I break the rules I might not be allowed to use a computer/tablet

Signed (child):

(The school will need to decide whether or not they wish the children to sign the agreement – and at which age - for younger children the signature of a parent/carer should be sufficient)

Signed (parent):

Primary schools using this acceptable use agreement for younger children may also wish to use (or adapt for use) the Parent/Carer Acceptable Use Agreement (the template can be found later in these templates) as this provides additional permission forms (including the digital and video images permission form).

# Parent/Carer Acceptable Use Agreement Template

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies provide powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

### This Acceptable Use Policy is intended to ensure

* that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
* that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
* that parents and carers are aware of the importance of online safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that *students/pupils* will have good access to digital technologies to enhance their learning and will, in return, expect the *students/pupils* to agree to be responsible users. A copy of the *Student/Pupil* Acceptable Use Policy is attached to this permission form, so that parents/carers will be aware of the school expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school’s work. (Schools will need to decide whether or not they wish parents to sign the Acceptable Use Agreement on behalf of their child)

## Permission Form

Parent/Carers Name:

Student/Pupil Name:

As the parent/carer of the above *students/pupils*, I give permission for my son/daughter to have access to the internet and to ICT systems at school.

Either: (KS2 and above)

I know that my son/daughter has signed an Acceptable Use Agreement and has received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

Or: (KS1)

I understand that the school has discussed the Acceptable Use Agreement with my son/daughter and that they have received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son’s/daughter’s activity on the systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child’s online safety.

As the school is collecting personal data by issuing this form, it should inform parents/carers as to:

* This form (electronic or printed)
* Who will have access to this form
* Where this form will be stored
* How long this form will be stored for
* How this form will be destroyed

Signed:

Date:

# Use of Digital/Video Images

The use of digital/video images plays an important part in learning activities. *Students/Pupils* and members of staff may use digital cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons.

Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media. Where an image is publicly shared by any means, only your child’s *\*delete as relevant\** first name/initials will be used.

The school will comply with the Data Protection Act and request parent’s/carers permission before taking images of members of the school. We will also ensure that when images are published that the young people cannot be identified by the use of their names.

In accordance with guidance from the Information Commissioner’s Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone’s privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other *students/pupils* in the digital/video images.

Parents/carers are requested to sign the permission form below to allow the school to take and use images of their children and for the parents/carers to agree.

As the school is collecting personal data by issuing this form, it should inform parents/carers as to:

#### This Form (electronic or printed)

* Who will have access to this form
* Where this form will be stored
* How long this form will be stored for
* How this form will be destroyed

#### The Images

* Where the images may be published. Such as; Twitter, Facebook, the school website, local press, etc. (see relevant section of form below)
* Who will have access to the images
* Where the images will be stored
* How long the images will be stored for
* How the images will be destroyed
* How a request for deletion of the images can be made

## Digital/Video Images Permission Form

Parent/Carers Name: Student/Pupil Name:

|  |  |
| --- | --- |
| As the parent/carer of the above student/pupil, I agree to the school taking digital/video images of my child/children. | Yes/No |
| I agree to these images being used: |  |
| to support learning activities. | Yes/No |
| in publicity that reasonably celebrates success and promotes the work of the school. | Yes/No |
| Insert statements here that explicitly detail where images are published by the school  | Yes/No |
| I agree that if I take digital or video images at, or of school events which include images of children, other than my own, I will abide by these guidelines in my use of these images.  | Yes/No |

Signed:

Date:

# Use of Cloud Systems Permission Form

Schools that use cloud hosting services may be required to seek parental permission to set up an account for pupils/students.

Schools will need to review and amend the section below, depending on which cloud hosted services are used.

The school uses *\*insert cloud service provider name\** for *pupils/students* and staff. This permission form describes the tools and pupil/student responsibilities for using these services.

The following services are available to each *pupil/student* as part of the school’s online presence in *\*insert cloud service provider name\**

Using *\*insert cloud service provider name\** will enable your child to collaboratively create, edit and share files and websites for school related projects and communicate via email with other pupils and members of staff. These services are entirely online and available 24/7 from any internet-connected computer.

The school believes that use of the tools significantly adds to your child’s educational experience.

As the school is collecting personal data and sharing this with a third party, it should inform parents/carers about:

#### This Form (electronic or printed)

* Who will have access to this form
* Where this form will be stored
* How long this form will be stored for
* How this form will be destroyed

#### The Data Shared with the Service Provider

* What data will be shared
* Who the data will be shared with
* Who will have access to the data
* Where the data will be stored
* How long the data will be stored for
* How the data will be destroyed
* How a request for deletion of the data can be made

|  |  |
| --- | --- |
| Do you consent to your child to having access to this service?  | Yes/No |

Student/Pupil Name: Parent/Carers Name:

Signed: Date:

# Use of Biometric Systems

If the school uses biometric systems (e.g. fingerprint/palm recognition technologies) to identify children for access, attendance recording, charging, library lending etc. it may be required, or choose to seek permission from a parent or carer.

The school uses biometric systems for the recognition of individual children in the following ways (the school should describe here how it uses the biometric system).

Biometric technologies have certain advantages over other automatic identification systems as pupils do not need to remember to bring anything with them (to the canteen or school library) so nothing can be lost, such as a swipe card. The school has carried out a data privacy impact assessment and is confident that the use of such technologies is effective and justified in a school context.

No complete images of fingerprints/palms are stored and the original image cannot be reconstructed from the data. Meaning that it is not possible, for example, to recreate a pupil's fingerprint or even the image of a fingerprint from what is in effect a string of numbers.

As the school is collecting special category personal data and *\*delete as appropriate\** sharing this with a third party, it should inform parents/carers about:

#### This Form (electronic or printed)

* Who will have access to this form
* Where this form will be stored
* How long this form will be stored for
* How this form will be destroyed

#### The Data Shared with the Service Provider

* What data will be shared
* Who the data will be shared with
* Who will have access to the data
* Where the data will be stored
* How long the data will be stored for
* How the data will be destroyed
* How consent to process the biometric data can be withdrawn

Parent/Carers Name:

Student/Pupil Name:

|  |  |
| --- | --- |
| As the parent/carer of the above student/pupil, I agree to the school using biometric recognition systems, as described above. | Yes/No |
| I understand that the images cannot be used to create a whole fingerprint/palm print of my child and that these images will not be shared with anyone outside the school. | Yes/No |

Signed:

### Student/Pupil Acceptable Use Agreement

On the following pages we have copied, for the information of parents and carers, the Student/Pupil Acceptable Use Agreement.

It is suggested that when the Student/Pupil AUP is written that a copy should be attached to the Parents/Carers Acceptable Use Agreement to provide information for parents and carers about the rules and behaviours that students/pupils have committed to by signing the form.

# Staff (and Volunteer) Acceptable Use Policy Agreement Template

Sections that include advice or guidance are written in BLUE. It is anticipated that schools will remove these sections from their final document. Schools should review and amend the contents of this agreement to ensure that it is consistent with their Online Safety Policy and other relevant school policies. Due to the number of optional statements and the advice/guidance sections included in this template, it is anticipated that the final AUP will be more concise.

## School Policy

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 information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

### This Acceptable Use Policy is intended to ensure

* that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
* that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
* that staff are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for *students/pupils* learning and will, in return, expect staff and volunteers to agree to be responsible users.

## Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that students/pupils receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

### For my professional and personal safety

* I understand that the *school* will monitor my use of the school digital technology and communications systems.
* I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, VLE etc.) out of school, and to the transfer of personal data (digital or paper based) out of school (schools should amend this section in the light of their policies which relate to the use of school systems and equipment out of school)
* I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school. (schools should amend this section in the light of their policies which relate to the personal use, by staff and volunteers, of school systems)
* I will not disclose my username or password to anyone else, nor will I try to use any other person’s username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
* I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

28

### I will be professional in my communications and actions when using *school* systems

* I will not access, copy, remove or otherwise alter any other user’s files, without their express permission.
* I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
* I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school’s policy on the use of digital/video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website/VLE) it will not be possible to identify by name, or other personal information, those who are featured.
* I will only use social networking sites in school in accordance with the school’s policies. (schools should amend this section to take account of their policy on access to social networking and similar sites)
* I will only communicate with students/pupils and parents/carers using official school systems. Any such communication will be professional in tone and manner. (schools should amend this section to take account of their policy on communications with students/pupils and parents/carers. Staff should be made aware of the risks attached to using their personal email addresses/mobile phones/social networking sites for such communications)
* I will not engage in any on-line activity that may compromise my professional responsibilities.

### The school has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the *school*

* When I use my mobile devices in school, I will follow the rules set out in this agreement, in the same way as if I was using *school* equipment. I will also follow any additional rules set by the *school* about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses. (schools should amend this section in the light of their policies which relate to the use of staff devices)
* I will not use personal email addresses on the school ICT systems. (schools should amend this section in the light of their email policy – some schools will choose to allow the use of staff personal email addresses on the premises).
* I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
* I will ensure that my data is regularly backed up, in accordance with relevant school policies.
* I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist or extremist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
* I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
* I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies. (schools should amend this section in the light of their policies on installing programmes/altering settings)
* I will not disable or cause any damage to school equipment, or the equipment belonging to others.
* I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Personal Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based documents containing personal data must be held in lockable storage.
* I understand that data protection policy requires that any staff or student/pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
* I will immediately report any damage or faults involving equipment or software, however this may have happened.

### When using the internet in my professional capacity or for school sanctioned personal use

* I will ensure that I have permission to use the original work of others in my own work
* Where work is protected by copyright, I will not download or distribute copies (including music and videos).

### I understand that I am responsible for my actions in and out of the *school*

* I understand that this Acceptable Use Policy applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school
* I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include (schools should amend this section to provide relevant sanctions as per their behaviour policies) a warning, a suspension, referral to a further body (to be named) and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff/Volunteer Name:

Signed:

Date:

# Acceptable Use Agreement for Community Users Template

#### This Acceptable Use Agreement is intended to ensure

* that community users of school digital technologies will be responsible users and stay safe while using these systems and devices
* that school systems, devices and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
* that users are protected from potential harm in their use of these systems and devices

## Acceptable Use Agreement

I understand that I must use school systems and devices in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems, devices and other users. This agreement will also apply to any personal devices that I bring into the school:

* I understand that my use of school systems and devices and digital communications will be monitored
* I will not use a personal device that I have brought into school for any activity that would be inappropriate in a school setting.
* I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist and extremist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
* I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

28

* I will not access, copy, remove or otherwise alter any other user’s files, without permission.
* I will ensure that if I take and/or publish images of others I will only do so with their permission. I will not use my personal equipment to record these images, without permission. If images are published it will not be possible to identify by name, or other personal information, those who are featured.
* I will not publish or share any information I have obtained whilst in the school on any personal website, social networking site or through any other means, unless I have permission from the school.
* I will not, without permission, make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
* I will not install or attempt to install programmes of any type on a school device, nor will I try to alter computer settings, unless I have permission to do so.
* I will not disable or cause any damage to school equipment, or the equipment belonging to others.
* I will immediately report any damage or faults involving equipment or software, however this may have happened.
* I will ensure that I have permission to use the original work of others in my own work
* Where work is protected by copyright, I will not download or distribute copies (including music and videos).
* I understand that if I fail to comply with this Acceptable Use Agreement, the school has the right to remove my access to school systems/devices

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

As the school is collecting personal data by issuing this form, it should inform community users about:

* Who will have access to this form
* Where this form will be stored
* How long this form will be stored for
* How this form will be destroyed

Name: Signed:

Date:

# Responding to Incidents of Misuse – Flow Chart



# Record of Reviewing Devices/Internet Sites

Group:

Date:

Reason for investigation:

### Details of First Reviewing Person

Name:

Position:

Signature:

### Details of Second Reviewing Person

Name:

Position:

Signature:

### Name and Location of Computer Used for Review (For Websites)

####

|  |  |
| --- | --- |
| Website(s) address/device | Reason for Concern |
|  |  |
|  |  |
|  |  |

### Conclusion and Action Proposed or Taken

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

|  |
| --- |
| Reporting LogGroup:  |
| Date | Time | Incident | Action Taken | Incident Reported By | Signature |
| What? | By Whom? |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
| Training Needs Audit LogGroup:  |
| Relevant Training the Last 12 Months | Identified Training Need | To be Met By | Cost | Review Date |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

# School Technical Security Policy Template (including filtering and passwords)

### Suggestions for Use

Within this template sections which include information or guidance are shown in BLUE. It is anticipated that schools would remove these sections from their completed policy document, though this will be a decision for the group that produces the policy.

Where sections in the template are written in italics it is anticipated that schools would wish to consider whether or not to include that section or statement in their completed policy.

**Where sections are highlighted in BOLD text, it is the view of the SWGfL Online Safety Group that these would be an essential part of a school online safety policy.**

The template uses various terms such as school; students/pupils. Users will need to choose which term to use for their circumstances and delete the other accordingly.

## Introduction

Effective technical security depends not only on technical measures, but also on appropriate policies and procedures and on good user education and training. The school will be responsible for ensuring that the *school infrastructure/network* is as safe and secure as is reasonably possible and that:

* users can only access data to which they have right of access
* no user should be able to access another’s files (other than that allowed for monitoring purposes within the school’s policies).
* access to personal data is securely controlled in line with the school’s personal data policy
* logs are maintained of access by users and of their actions while users of the system
* there is effective guidance and training for users
* there are regular reviews and audits of the safety and security of school computer systems
* there is oversight from senior leaders and these have impact on policy and practice.

If the school has a managed ICT service provided by an outside contractor, it is the responsibility of the school to ensure that the managed service provider carries out all the online safety measures that might otherwise be carried out by the school itself (as suggested below). It is also important that the managed service provider is fully aware of the school Online Safety Policy/Acceptable Use Agreements). The school should also check other relevant body policies/guidance on these technical issues.

## Responsibilities

**The management of technical security will be the responsibility of** (insert title) (schools will probably choose the Network Manager/Technical Staff/Head of Computing or other relevant responsible person)

## Technical Security

### Policy Statements

**The school will be responsible for ensuring that their 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 receive guidance and training and will be effective in carrying out their responsibilities:**

* **school technical systems will be managed in ways that ensure that the school meets recommended technical requirements (if not managed by the Local Authority, these may be outlined in Local Authority/other relevant body technical/online safety policy and guidance)**
* **there will be regular reviews and audits of the safety and security of school technical systems**
* **servers, wireless systems and cabling must be securely located and physical access restricted**
* **appropriate security measures are in place to protect the servers, firewalls, switches, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data**
* **responsibilities for the management of technical security are clearly assigned to appropriate and well trained staff (this may be at school, local authority or managed provider level)**
* **all users will have clearly defined access rights to school technical systems. *Details of the access rights available to groups of users will be recorded by the network manager/technical staff/other person and will be reviewed, at least annually, by the online safety group.***
* **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***(see password section below)*
* (insert name or role) is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations (Inadequate licencing could cause the school to breach the Copyright Act which could result in fines or unexpected licensing costs)
* *mobile device security and management procedures are in place* (where mobile devices are allowed access to school systems). (schools/colleges may wish to add details of the mobile device security procedures that are in use).
* *school /local authority/managed service provider/technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the acceptable use agreement.* (schools/colleges may wish to add details of the monitoring programmes that are used)
* *remote management tools are used by staff to control workstations and view users activity*
* *an appropriate system is in place* (to be described) *for users to report any actual/potential technical incident to the online safety co-ordinator/network manager/technician (or other relevant person, as agreed)*
* an agreed policy is in place (to be described) for the provision of temporary access of “guests”, (e.g. trainee teachers, supply teachers, visitors) onto the school system
* *an agreed policy is in place* (to be described) *regarding the downloading of executable files and the installation of programmes on school devices by users*
* *an agreed policy is in place* (to be described) *regarding the extent of personal use that users (staff/learners/community users) and their family members are allowed on school devices that may be used out of school*
* an agreed policy is in place (to be described) regarding the use of removable media (eg memory sticks/CDs/DVDs) by users on school devices (see school personal data policy template in the appendix for further detail)
* the school infrastructure and individual workstations are protected by up to date software to protect against malicious threats from viruses, worms, trojans etc.

### personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured. (see school personal data policy template in the appendix for further detail)

## Password Security

A safe and secure username/password system is essential if the above is to be established and will apply to all school technical systems, including networks, devices, email and learning platform). You can find out more about passwords, why they are important and how to manage them in our blog article. You may wish to share this with staff members to help explain the significance of passwords as this is helpful in explaining why they are necessary and important. Where sensitive data is in use – particularly when accessed on mobile devices – schools may wish to use more secure forms of authentication e.g. two factor authentication.

Further guidance can be found from the [National Cyber Security Centre](https://www.ncsc.gov.uk/collection/passwords) and [SWGfL “Password](https://swgfl.org.uk/resources/password-management-and-security-guide/) Management & Security Guide”

### Policy Statements

* **These statements apply to all users.**
* **All school networks and systems will be protected by secure passwords.**
* **All users have clearly defined access rights to school technical systems and devices. 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, by the online safety group (or other group).**
* **All users (adults and students/pupils) have responsibility 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.**
* **Passwords must not be shared with anyone.**
* **All users** **will be provided with a username and password** by xxxxx (insert name or title) (see section on password generation in technical notes) who will keep an up to date record of users and their usernames.

## Password Requirements

* **Passwords should be long. Good practice highlights that passwords over 12 characters in length are considerably more difficult to compromise than shorter passwords. Passwords generated by using a combination of unconnected words that are over 16 characters long are extremely difficult to crack. Password length trumps any other special requirements such as uppercase/lowercase letters, number and special characters. Passwords should be easy to remember, but difficult to guess or crack.**
* **Passwords should be different for different accounts, to ensure that other systems are not put at risk if one is compromised and should be different for systems used inside and outside of school**
* **Passwords must not include names or any other personal information about the user that might be known by others**
* **Passwords must be changed on first login to the system**
* *The school may wish to recommend to staff and students/pupils (depending on age) that they make use of a ‘password vault’ these can store passwords in an encrypted manner and can generate very difficult to crack passwords. There may be a charge for these services.*
* *Passwords should not be set to expire as long as they comply with the above, but should be unique to each service the user logs into.*

## Learner Passwords

Primary schools will need to decide at which point they will allocate individual usernames and passwords to pupils. They may choose to use class logons for younger children (under 9) - though increasingly children are using their own passwords to access programmes out of school. Schools need to be aware of the risks associated with not being able to identify any individual who may have infringed the rules set out in the policy and the Acceptable Use Agreement (AUA). Use by students/pupils in this way should always be supervised and members of staff should never use a class log on for their own network/internet access. Schools should also consider the implications of using whole class logons when providing access to learning environments and applications, which may be used outside school.

* **Records of learner usernames and passwords for younger students/pupils can be kept in an electronic or paper-based form, but they must be securely kept when not required by the user.** *Password complexity in foundation phase should be reduced (for example 6-character maximum) and should not include special characters. Where external systems have different password requirements the use of random words or sentences should be encouraged.*
* Password requirements for older students/pupils and should increase as students’/pupils progress through school.
* Users will be required to change their password if it is compromised. Some schools may choose to reset passwords at the start of each academic year to avoid large numbers of forgotten password reset requests where there is no user-controlled reset process. (Note: passwords should not be regularly changed but should be secure and unique to each account.)
* Students/pupils will be taught the importance of password security, this should include how passwords are compromised, and why these password rules are important.

Schools/colleges may wish to add to this list for all or some students/pupils any of the relevant policy statements from the staff section above.

## Notes for Technical Staff/Teams

* **Each administrator should have an individual administrator account, as well as their own user account with access levels set at an appropriate level. Consideration should also be given to using two factor authentication for such accounts.**
* **An administrator account password for the school systems should also be kept in a secure place e.g. school safe. This account and password should only be used to recover or revoke access. Other administrator accounts should not have the ability to delete this account*. (A school should never allow one user to have sole administrator access)***
* **Any digitally stored administrator passwords should be hashed using a suitable algorithm for storing passwords (e.g. Bcrypt or Scrypt). Message Digest algorithms such as MD5, SHA1, SHA256 etc. should not be used.**
* *It is good practice that where passwords are used there is a user-controlled password reset process to enable independent, but secure re-entry to the system. This ensures that only the owner has knowledge of the password.*
* Where user-controlled reset is not possible, passwords for new users, and replacement passwords for existing users will be allocated by xxxxx (insert title) (schools may wish to have someone other than the school’s technical staff carrying out this role e.g. an administrator who is easily accessible to users). Good practice is that the password generated by this change process should be system generated and only known to the user. This password should be temporary and the user should be forced to change their password on first login. The generated passwords should also be long and random.
* *Where automatically generated passwords are not possible, then a good password generator should be used by* xxxxx (insert title) *to provide the user with their initial password. There should be a process for the secure transmission of this password to limit knowledge to the password creator and the user. The password should be temporary and the user should be forced to change their password on the first login.*
* *Requests for password changes should be authenticated* by (the responsible person) *to ensure that the new password can only be passed to the genuine* user (the school will need to decide how this can be managed – possibly by requests being authorised by a line manager for a request by a member of staff or by a member of staff for a request by a learner)
* **Suitable arrangements should be in place to provide visitors with appropriate access to systems which expires after use.** *(For example, your technical team may provide pre-created user/password combinations that can be allocated to visitors, recorded in a log, and deleted from the system after use.)*
* **In good practice, the account is “locked out” following six successive incorrect log-on attempts.**
* **Passwords shall not be displayed on screen, and shall be securely hashed when stored (use of one-way encryption).**

## Training/Awareness

It is essential that users should be made aware of the need for keeping passwords secure, and the risks attached to unauthorised access/data loss. This should apply to even the youngest of users. It is also essential that users be taught how passwords are compromised, so they understand why things should be done a certain way. Please see our blog for more details on this.

### Members of staff will be made aware of the school ’s password policy

* at induction
* through the school ’s online safety policy and password security policy
* through the acceptable use agreement

### Students/pupils will be made aware of the school’s/college’s password policy

* in lessons (the school should describe how this will take place)
* through the Acceptable Use Agreement

### Audit/Monitoring/Reporting/Review

The responsible person (insert title) will ensure that full records are kept of:

* User Ids and requests for password changes
* *User logons*
* *Security incidents related to this policy*

# Filtering

36

## Introduction

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so, because the content on the web changes dynamically and new technologies are constantly being developed. It is important, therefore, to understand that filtering is only one element in a larger strategy for online safety and acceptable use. It is important that the school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.

Many users are not aware of the flexibility provided by many filtering services at a local level for schools. Where available, schools should use this flexibility to meet their learning needs and reduce some of the frustrations occasionally felt by users who wish to maximise the use of the new technologies.

Schools need to consider carefully the issues raised and decide:

* Whether they will use the provided filtering service without change or to allow flexibility for sites to be added or removed from the filtering list for their organisation
* Whether to introduce differentiated filtering for different groups/ages of users
* Whether to remove filtering controls for some internet use (e.g. social networking sites) at certain times of the day or for certain users
* Who has responsibility for such decisions and the checks and balances put in place
* What other system and user monitoring systems will be used to supplement the filtering system and how these will be used

Guidance on “appropriate filtering”. can be found on the [UK Safer Internet Centre site](https://www.saferinternet.org.uk/advice-centre/teachers-and-school-staff/appropriate-filtering-and-monitoring).

Schools may wish to test their filtering for protection against illegal materials at: [SWGfL Test Filtering](http://testfiltering.com)

## Responsibilities

The responsibility for the management of the school’s filtering policy will be held by (insert title). They will manage the school filtering, in line with this policy and will keep records/logs of changes and of breaches of the filtering systems.

To ensure that there is a system of checks and balances and to protect those responsible, changes to the school filtering service must (schools should choose their relevant responses):

* **be logged in change control logs**
* **be reported to a second responsible person** (insert title):
* *either... be reported to and authorised by a second responsible person prior to changes being made* (recommended)
* *or... be reported to a second responsible person* (insert title) *every X weeks/months in the form* of *an audit of the change control logs*
* *be reported to the Online Safety Group every X weeks/months in the form of an audit of the change control logs*

All users have a responsibility to report immediately to (insert title) any infringements of the school’s filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.

Users must not attempt to use any programmes or software that might allow them to bypass the filtering/security systems in place to prevent access to such materials.

## Policy Statements

Internet access is filtered for all users. Differentiated internet access is available for staff and customised filtering changes are managed by the school. Illegal content is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and other illegal content lists. Filter content lists are regularly updated and internet use is logged and frequently monitored. The monitoring process alerts the school to breaches of the filtering policy, which are then acted upon. There is a clear route for reporting and managing changes to the filtering system. Where personal mobile devices are allowed internet access through the school network, filtering will be applied that is consistent with school practice.

* *Either - The school maintains and supports the managed filtering service provided by the Internet Service Provider* (or other filtering service provider)
* *Or – The school manages its own filtering service* (N.B. If a school decides to remove the external filtering and replace it with another internal filtering system, this should be clearly explained in the policy and evidence provided that the Headteacher/Principal would be able to show, in the event of any legal issue that the school was able to meet its statutory requirements to ensure the safety of staff/students/pupils)
* *The school has provided enhanced/differentiated user-level filtering through the use of the* (insert name) *filtering programme. (allowing different filtering levels for different ages/stages and different groups of users – staff/pupils/students etc.)*
* *In the event of the technical staff 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/Principal (or other nominated senior leader).*
* *Mobile devices that access the school internet connection (whether school or personal devices) will be subject to the same filtering standards as other devices on the school systems*
* *Any filtering issues should be reported immediately to the filtering provider.*
* *Requests from staff for sites to be removed from the filtered list will be considered by the technical staff (*insert name or title) (N.B. an additional person should be nominated – to ensure protection for the Network Manager or any other member of staff, should any issues arise re unfiltered access). *If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the Online Safety Group.*

## Education/Training/Awareness

*Pupils/students* will be made aware of the importance of filtering systems through the online safety education programme (schools may wish to add details). They will also be warned of the consequences of attempting to subvert the filtering system.

Staff users will be made aware of the filtering systems through: (amend as relevant)

* the Acceptable Use Agreement
* induction training
* staff meetings, briefings, Inset.

Parents will be informed of the school’s filtering policy through the Acceptable Use Agreement and through online safety awareness sessions/newsletter etc. (amend as relevant)

## Changes to the Filtering System

In this section the school should provide a detailed explanation of:

* how, and to whom, users may request changes to the filtering (whether this is carried out in school or by an external filtering provider)
* the grounds on which they may be allowed or denied (schools may choose to allow access to some sites e.g. social networking sites for some users, at some times, or for a limited period of time. There should be strong educational reasons for changes that are agreed).
* how a second responsible person will be involved to provide checks and balances (preferably this will be at the time of request, but could be retrospectively through inspection of records/audit of logs)
* any audit/reporting system

Users who gain access to, or have knowledge of others being able to access, sites which they feel should be filtered (or unfiltered) should report this in the first instance to (insert title) who will decide whether to make school level changes (as above).

# Monitoring

Some schools supplement their filtering systems with additional monitoring systems. If this is the case, schools should include information in this section, including – if they wish – details of internal or commercial systems that are in use. They should also ensure that users are informed that monitoring systems are in place.

No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network and on school equipment as indicated in the School Online Safety Policy and the Acceptable Use Agreement. *Monitoring will take place as follows:* (details should be inserted if the school so wishes).

## Audit/Reporting

Logs of filtering change controls and of filtering incidents will be made available to: (schools should amend as relevant)

* the second responsible person (insert title)
* Online Safety Group
* Online Safety Governor/Governors committee
* External Filtering provider/Local Authority/Police on request

The filtering policy will be reviewed in the response to the evidence provided by the audit logs of the suitability of the current provision. (The evidence might show a large number of requests to remove the filtering from sites – in which case schools might question whether their current level of filtering is too restrictive for educational purposes. Alternatively, a large number of incidents where users try to subvert the filtering system might suggest that improved monitoring/disciplinary action might be necessary).

[Somerset Guidance for schools – questions for technical support](https://www.somerset.org.uk/sites/edtech/eSafety/Leading/Questions%20for%20Technical%20Support%202018.pdf)  – this checklist is particularly useful where a school uses external providers for its technical support/security.

SWGfL provides a site for schools to test their filtering to ensure that illegal materials cannot be accessed: [SWGfL Test Filtering](http://testfiltering.com/)

# School Personal Data Advice and Guidance

### Suggestions for Use

This document is for advice and guidance purposes only. It is anticipated that schools / colleges will use this advice alongside their own data protection policy. This document is not intended to provide legal advice and the school/college is encouraged to seek their own legal counsel when considering their management of personal data.

The template uses the terms students/pupils to refer to the children or young people at the institution.

## School Personal Data Handling

Recent publicity about data breaches suffered by organisations and individuals continues to make the area of personal data protection a current and high profile issue for schools, academies and other organisations. It is important that the school has a clear and well understood personal data handling policy in order to minimise the risk of personal data breaches. A breach may arise from a theft, a deliberate attack on your systems, the unauthorised or malicious use of personal data by a member of staff, accidental loss, or equipment failure. In addition:

* no school or individual would want to be the cause of a data breach, particularly as the impact of data loss on individuals can be severe, put individuals at risk and affect personal, professional or organisational reputation
* schools/colleges are “data rich” and the introduction of electronic storage and transmission of data has created additional potential for the loss of data
* the school will want to avoid the criticism and negative publicity that could be generated by anypersonal data breach
* the school is subject to a wide range of legislation related to data protection and data use, with significant penalties for failure to observe the relevant legislation
* it is a legal requirement for all schools to have a Data Protection Policy and be able to demonstrate compliance with data protection law.

Schools have always held personal data on the pupils in their care, and increasingly this data is held digitally and accessible not just in the school but also from remote locations. It is important to stress that the data protection laws apply to all forms of personal data, regardless of whether it is held on paper or in electronic format. However, as it is part of an overall online safety policy template, this document will place particular emphasis on data which is held or transferred digitally.

Schools will need to carefully review their policy, in the light of pertinent local/external regulations and guidance and changes in legislation.

## Introduction

Schools and their employees must do everything within their power to ensure the safety and security of any material of a personal or sensitive nature, including personal data.

It is the responsibility of all members of the school community to take care when handling, using or transferring personal data, that it cannot be accessed by anyone who does not:

* have permission to access that data
* need to have access to that data.

Data breaches can have serious effects on individuals and/or institutions concerned, can bring the school into disrepute and may well result in disciplinary action, criminal prosecution and fines imposed by the Information Commissioner. Particularly, all transfer of data is subject to risk of loss or contamination.

Anyone who has access to personal data must know, understand and adhere to the relevant school policy which brings together the statutory requirements contained in relevant data protection legislation and relevant regulations and guidance.

38

## Personal Data

The school and its employees will have access to a wide range of personal information and data. The data may be held in a digital format or on paper records. Personal data is information that relates to an identified or identifiable living individual This will include:

* personal information about members of the school community – including students/pupils, members of staff and parents/carers e.g. names, addresses, contact details, legal guardianship contact details, health records, disciplinary records
* curricular / academic data e.g. class lists, student/pupil progress records, reports, references
* professional records e.g. employment history, taxation and national insurance records, appraisal records and references
* any other information that might be disclosed by parents/carers or by other agencies working with families or staff members.

## Data Protection Impact Assessments

Data Protection Impact Assessments identify and address privacy risks early on in any project so that you can mitigate them before the project goes live.

DPIAs should be carried out by Data Managers (where relevant) under the support and guidance of the DPO. Ideally you should conduct a DPIA before processing activity starts. However, some may need to be retrospective in the early stages of compliance activity.

The risk assessment will involve:

* recognising the risks that are present
* judging the level of the risks (both the likelihood and consequences)
* prioritising the risks.

A DPIA should contain:

* a description of the processing operations and the purpose
* an assessment of the necessity and proportionality of the processing in relation to the purpose
* an assessment of the risks to individuals
* the measures in place to address risk, including security and to demonstrate that you comply.

Or more simply and fully:

* who did you talk to about this?
* what is going to happen with the data and how – collection, storage, usage, disposal
* how much personal data will be handled (number of subjects)
* why you need use personal data in this way
* what personal data (including if it’s in a ‘special category’) are you using
* at what points could the data become vulnerable to a breach (loss, stolen, malicious)
* what are the risks to the rights of the individuals if the data was breached
* what are you going to do in order to reduce the risks of data loss and prove you are compliant with the law.

DPIA is an ongoing process and should be re-visited at least annually to verify that nothing has changed since the processing activity started.

## Secure Storage Of and Access to Data

The school should ensure that systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them. Access to protected data will be controlled according to the role of the user. Members of staff will not, as a matter of course, be granted access to the whole management information system.

[Good practice](https://www.ncsc.gov.uk/guidance/password-guidance-simplifying-your-approach) suggests that all users will use strong passwords made up from a combination of simpler words. User passwords must never be shared.

Personal data may only be accessed on machines that are securely protected. Any device that can be used to access personal data must be locked if left (even for very short periods) and set to auto lock if not used for five minutes.

All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.

Personal data should only be stored on school equipment. Private equipment (i.e. owned by the users) must not be used for the storage of school personal data.

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
* The device must offer approved virus and malware checking software
* The data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete.

The school will need to set its own policy as to whether data storage on removal media is allowed, even if encrypted. Some organisations do not allow storage of personal data on removable devices.

The school should have a clear policy and procedures for the automatic backing up, accessing and restoring of all data held on school systems, including off-site backups.

The school should have clear policy and procedures for the use of “Cloud Based Storage Systems” (for example Dropbox, Microsoft 365, Google Drive) and is aware that data held in remote and cloud storage is still required to be protected in line with the Data Protection Act. The school will ensure that it is satisfied with controls put in place by remote / cloud based data services providers to protect the data.

As a Data Controller, the school is responsible for the security of any data passed to a “third party”. Data Protection clauses must be included in all contracts where personal data is likely to be passed to a third party.

All paper based personal data must be held in lockable storage, whether on or off site.

## Secure Transfer of Data and Access Out of School

The school recognises that personal data may be accessed by users out of school or transferred to other agencies. In these circumstances:

* Users may not remove or copy sensitive or restricted or protected personal data from the school or authorised premises without permission and unless the media is encrypted and password protected and is transported securely for storage in a secure location
* Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (e.g. family members) when out of school
* When restricted or protected personal data is required by an authorised user from outside the organisation’s premises (for example, by a member of staff to work from their home), they should preferably have secure remote access to the management information system or learning platform
* If secure remote access is not possible, users must only remove or copy personal or sensitive data from the organisation or authorised premises if the storage media, portable or mobile device is encrypted and is transported securely for storage in a secure location
* Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software
* Particular care should be taken if data is taken or transferred to another country and advice should be taken locally in this event.

## Disposal of Data

The school should implement a document retention schedule that defines the length of time data is held before secure destruction. The school must ensure the safe destruction of personal data when it is no longer required.

The disposal of personal data, in either paper or electronic form, must be conducted in a way that makes reconstruction highly unlikely. Electronic files must be securely disposed of, and other media must be shredded, incinerated or otherwise disintegrated.

A Destruction Log should be kept of all data that is disposed of. The log should include the document ID, classification, date of destruction, method and authorisation.

## Audit Logging / Reporting / Incident Handling

Where GDPR applies (within the EU), organisations are required to keep records of processing activity. This must include:

* the name and contact details of the data controller
* where applicable, the name and contact details of the joint controller and data protection officer
* the purpose of the processing
* to whom the data has been/will be disclosed
* description of data subject and personal data
* where relevant the countries it has been transferred to
* under which condition for processing the data has been collected
* under what lawful basis processing is being carried out
* where necessary, how it is retained and destroyed
* a general description of the technical and organisational security measures.

Clearly, in order to maintain these records good auditing processes must be followed, both at the start of the exercise and on-going throughout the lifetime of the requirement. Therefore, audit logs will need to be kept to:

* provide evidence of the processing activity and the DPIA
* record where, how and to whom data has been shared
* log the disposal and destruction of the data
* enable the school to target training at the most at-risk data
* record any breaches that impact on the data

## Data Breaches

If you experience a personal data breach you need to consider whether this poses a risk to people. You need to consider the likelihood and severity of any risk to people’s rights and freedoms, following the breach. When you’ve made this assessment, if it’s likely there will be a risk then you may be required to notify and external body/national agency

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

The school should have a policy for reporting, logging, managing and recovering from information risk incidents, which establishes a:

* “responsible person” for each incident
* communications plan, including escalation procedure
* plan of action for rapid resolution
* plan of action of non-recurrence and further awareness raising

## Data Mapping

The process of data mapping is designed to help schools identify with whom their data is being shared in order that the appropriate contractual arrangements can be implemented. If a third party is processing personal data on your behalf about your students/pupils, then this processor may have obligations on behalf of the school to ensure that processing takes place in compliance with relevant data protection laws.

## Data Subject’s Right of Access

The school will need to identify the rights of access given to data subjects within local data protection laws and describe these here:

### Responsibilities

It is recommended that schools should appoint a Data Protection Officer. They should have:

* expert knowledge
* timely and proper involvement in all issues relating to data protection
* the necessary resources to fulfil the role
* access to the necessary personal data processing operations
* a direct reporting route to the highest management level

The school may also wish to appoint a Data Manager. Schools/colleges are encouraged to separate this role from that of Data Protection Officer, where possible. This person will keep up to date with current legislation and guidance and will:

* determine and take responsibility for the school’s / college’s information risk policy and risk assessment
* oversee the System Controllers

The school may also wish to appoint System Controllers for the various types of data being held (e.g. learner information / staff information / assessment data etc.). These Controllers will manage and address risks to the information and will understand:

* what information is held, for how long and for what purpose
* how information has been amended or added to over time, and
* who has access to the data and why.

Everyone in the school has the responsibility of handling protected or sensitive data in a safe and secure manner.

### Training & Awareness

All staff should receive data handling awareness/data protection training and will be made aware of their responsibilities. This should be undertaken regularly. You can do this through:

* Induction training for new staff
* Staff meetings / briefings / training sessions
* Day to day support and guidance from System Controllers

# Mobile Technologies Policy Template (Inc. BYOD/BYOT)

37

Mobile technology devices may be a school owned/provided or privately owned smartphone, tablet, notebook/laptop or other technology that usually has the capability of utilising the school’s wireless network. The device then has access to the wider internet which may include the school’s learning platform and other cloud based services such as email and data storage.

The absolute key to considering the use of mobile technologies is that the pupils/students, staff and wider school community understand that the primary purpose of having their personal device at school is educational and that this is irrespective of whether the device is school owned/provided or personally owned. The mobile technologies policy should sit alongside a range of polices including but not limited to the Safeguarding Policy, Bullying Policy, Acceptable Use Policy, policies around theft or malicious damage and the Behaviour Policy. Teaching about the safe and appropriate use of mobile technologies should be included in the online safety education programme.

## Potential Benefits of Mobile Technologies

Research has highlighted the widespread uptake of mobile technologies amongst adults and children of all ages. Web-based tools and resources have changed the landscape of learning. Students now have at their fingertips unlimited access to digital content, resources, experts, databases and communities of interest. By effectively maximizing the use of such resources, schools not only have the opportunity to deepen student learning, but they can also develop digital literacy, fluency and citizenship in students/pupils that will prepare them for the high tech world in which they will live, learn and work.

## Considerations

There are a number of issues and risks to consider when implementing mobile technologies, these include; security risks in allowing connections to your school network, filtering of personal devices, breakages and insurance, access to devices for all students/pupils, avoiding potential classroom distraction, network connection speeds, types of devices, charging facilities, total cost of ownership

Schools may consider implementing the use of mobile technologies as a means of reducing expenditure on school provided devices. However, it is important to remember that the increased network management costs and overheads involved in implementing this properly are likely to counterbalance or outweigh any savings.

The use of mobile technologies brings both real benefits and challenges for the whole school community – including teachers - and the only effective way for a school to implement these successfully is to involve the whole school community from the outset. Before the school embarks on this path, the risks and benefits must be clearly identified and shared with all stakeholders.

A range of mobile technology implementations is possible. The school should consider the following statements and remove those that do not apply to their planned implementation approach.

* The school Acceptable Use Agreements for staff, pupils/students and parents/carers will give consideration to the use of mobile technologies
* The school allows: (the school should complete the table below to indicate which devices are allowed and define their access to school systems)

|  |  |  |
| --- | --- | --- |
|  | School / Devices | Personal Devices |
|  | School owned and allocated to a single user | School owned for use by multiple users | Authorised Device[[1]](#footnote-1) | Pupil / Student owned | Staff owned | Visitor owned |
| Allowed in school | Yes | Yes | Yes | Yes/No[[2]](#footnote-2) | Yes/No4 | Yes/No4 |
| Full network access | Yes | Yes | Yes |  |  |  |
| Internet only |  |  |  |  |  |  |
| No network access |  |  |  |  |  |  |

* **The school has provided technical solutions for the safe use of mobile technology for school devices/personal devices (delete/amend as appropriate):**
	+ **All school devices are controlled though the use of Mobile Device Management software**
	+ **Appropriate access control is applied to all mobile devices according to the requirements of the user (e.g. Internet only access, network access allowed, shared folder network access)**
	+ **The school has addressed broadband performance and capacity to ensure that core educational and administrative activities are not negatively affected by the increase in the number of connected devices**
	+ **For all mobile technologies, filtering will be applied to the internet connection and attempts to bypass this are not permitted**
	+ **Appropriate exit processes are implemented for devices no longer used at a school location or by an authorised user**. These may include; revoking the link between MDM software and the device, removing proxy settings, ensuring no sensitive data is removed from the network, uninstalling school-licenced software etc.
	+ *All school devices are subject to routine monitoring*
	+ *Pro-active monitoring has been implemented to monitor activity*
* *When personal devices are permitted:*
	+ *All personal devices are restricted through the implementation of technical solutions that provide appropriate levels of network access*
	+ *Personal devices are brought into the school entirely at the risk of the owner and the decision to bring the device in to the school lies with the user (and their parents/carers) as does the liability for any loss or damage resulting from the use of the device in school*
	+ *The school accepts no responsibility or liability in respect of lost, stolen or damaged devices while at school or on activities organised or undertaken by the school (the school recommends insurance is purchased to cover that device whilst out of the home)*
	+ *The school accepts no responsibility for any malfunction of a device due to changes made to the device while on the school network or whilst resolving any connectivity issues*
	+ *The school recommends that the devices are made easily identifiable and have a protective case to help secure them as the devices are moved around the school. Pass-codes or PINs should be set on personal devices to aid security*
	+ *The school is not responsible for the day to day maintenance or upkeep of the users personal device such as the charging of any device, the installation of software updates or the resolution of hardware issues*
* **Users are expected to act responsibly, safely and respectfully in line with current Acceptable Use Agreements, in addition;**
	+ **Devices may not be used in tests or exams**
	+ **Visitors should be provided with information about how and when they are permitted to use mobile technology in line with local safeguarding arrangements**
	+ **Users are responsible for keeping their device up to date through software, security and app updates. The device is virus protected and should not be capable of passing on infections to the network**
	+ **Users are responsible for charging their own devices and for protecting and looking after their devices while in the school**
	+ **Personal devices should be charged before being brought to the school as the charging of personal devices is not permitted during the school day**
	+ **Devices must be in silent mode on the school site and on school buses**
	+ **School devices are provided to support learning. It is expected that pupils/students will bring devices to the school as required.**
	+ **Confiscation and searching (England) - the school has the right to take, examine and search any device that is suspected of unauthorised use, either technical or inappropriate.**
	+ **The changing of settings (exceptions include personal settings such as font size, brightness, etc…) that would stop the device working as it was originally set up and intended to work is not permitted**
	+ **The software/apps originally installed by the school must remain on the school owned device in usable condition and be easily accessible at all times. From time to time the school may add software applications for use in a particular lesson. Periodic checks of devices will be made to ensure that users have not removed required apps**
	+ **The school will ensure that devices contain the necessary apps for school work. Apps added by the school will remain the property of the school and will not be accessible to students/pupils on authorised devices once they leave the school roll. Any apps bought by the user on their own account will remain theirs.**
	+ **Users should be mindful of the age limits for app purchases and use and should ensure they read the terms and conditions before use.**
	+ **Users must only photograph people with their permission. Users must only take pictures or videos that are required for a task or activity. All unnecessary images or videos will be deleted immediately**
	+ *Devices may be used in lessons in accordance with teacher direction*
	+ *Staff owned devices should not be used for personal purposes during teaching sessions, unless in exceptional circumstances*
	+ *Printing from personal devices will not be possible*

## Insurance

Schools that have implemented an authorised device approach (1:1 deployment) may wish to consider how they will insure these devices and should include details of the claims process in this policy.

# Social Media Policy Template

Social media (e.g. Facebook, Twitter, LinkedIn) is a broad term for any kind of online platform which enables people to directly interact with each other. However, some games, for example Minecraft or World of Warcraft and video sharing platforms such as You Tube have social media elements to them.

*The school* recognises the numerous benefits and opportunities which a social media presence offers. Staff, parents/carers and pupils/students are actively encouraged to find creative ways to use social media. However, there are some risks associated with social media use, especially around the issues of safeguarding, bullying and personal reputation. This policy aims to encourage the safe use of social media by *the school,* its staff, parents, carers and children.

## Scope

**This policy is subject to the schools Codes of Conduct and Acceptable Use Agreements.**

### This Policy

* **Applies to all staff and to all online communications which directly or indirectly, represent the school.**
* **Applies to such online communications posted at any time and from anywhere.**
* Encourages the safe and responsible use of social media through training and education
* Defines the monitoring of public social media activity pertaining to the school

The school respects privacy and understands that staff and pupils/students may use social media forums in their private lives. However, personal communications likely to have a negative impact on professional standards and/or the school’s reputation are within the scope of this policy.

**Professional communications are those made through official channels, posted on a school account or using the school name. All professional communications are within the scope of this policy.**

Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with, or impacts on, the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.

Personal communications which do not refer to or impact upon the school are outside the scope of this policy.

Digital communications with pupils/students are also considered. *Staff may use social media to communicate with learners via a school social media account for teaching and learning purposes but must consider whether this is appropriate and consider the potential implications.*

## Organisational Control

### Roles & Responsibilities

* **SLT**
	+ Facilitating training and guidance on Social Media use.
	+ Developing and implementing the Social Media policy
	+ Taking a lead role in investigating any reported incidents.
	+ Making an initial assessment when an incident is reported and involving appropriate staff and external agencies as required.
	+ Receive completed applications for Social Media accounts
	+ Approve account creation
* **Administrator/Moderator**
	+ Create the account following SLT approval
	+ Store account details, including passwords securely
	+ Be involved in monitoring and contributing to the account
	+ Control the process for managing an account after the lead staff member has left the organisation (closing or transferring)
* **Staff**
	+ Know the contents of and ensure that any use of social media is carried out in line with this and other relevant policies
	+ Attending appropriate training
	+ Regularly monitoring, updating and managing content he/she has posted via school accounts
	+ Adding an appropriate disclaimer to personal accounts when naming the school

## Process for Creating New Accounts

The school community is encouraged to consider if a social media account will help them in their work, e.g. a history department Twitter account, or a “Friends of the school” Facebook page. Anyone wishing to create such an account must present a business case to the Leadership Team which covers the following points: -

* The aim of the account
* The intended audience
* How the account will be promoted
* Who will run the account (at least two staff members should be named)
* Will the account be open or private/closed

Following consideration by the SLT an application will be approved or rejected. In all cases, the SLT must be satisfied that anyone running a social media account on behalf of the school has read and understood this policy and received appropriate training. This also applies to anyone who is not directly employed by the school, including volunteers or parents.

## Monitoring

**School accounts must be monitored regularly and frequently** (preferably 7 days a week, including during holidays). Any comments, queries or complaints made through those accounts must be responded to within 24 hours (or on the next working day if received at a weekend) even if the response is only to acknowledge receipt. Regular monitoring and intervention is essential in case a situation arises where bullying or any other inappropriate behaviour arises on a school social media account.

### Behaviour

* **The school requires that all users using social media adhere to the standard of behaviour as set out in this policy and other relevant policies.**
* **Digital communications by staff must be professional and respectful at all times and in accordance with this policy**. Staff will not use social media to infringe on the rights and privacy of others or make ill-considered comments or judgments about staff. School social media accounts must not be used for personal gain. Staff must ensure that confidentiality is maintained on social media even after they leave the employment of the school.
* Users must declare who they are in social media posts or accounts. Anonymous posts are discouraged in relation to school activity.
* If a journalist makes, contact about posts made using social media staff must follow the school media policy before responding.
* Unacceptable conduct, (e.g. defamatory, discriminatory, offensive, harassing content or a breach of data protection, confidentiality, copyright) will be considered extremely seriously by the school and will be reported as soon as possible to a relevant senior member of staff, and escalated where appropriate.
* The use of social media by staff while at work may be monitored, in line with school policies. *The school permits reasonable and appropriate access to private social media sites. However, where excessive use is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken*
* The school will take appropriate action in the event of breaches of the social media policy. Where conduct is found to be unacceptable, the school will deal with the matter internally. Where conduct is considered illegal, the school will report the matter to the police and other relevant external agencies, and may take action according to the disciplinary policy.

### Legal Considerations

* **Users of social media should consider the copyright of the content they are sharing and, where necessary, should seek permission from the copyright holder before sharing.**
* **Users must ensure that their use of social media does not infringe upon relevant data protection laws, or breach confidentiality.**

### Handling Abuse

* When acting on behalf of the school, handle offensive comments swiftly and with sensitivity.
* If a conversation turns and becomes offensive or unacceptable, school users should block, report or delete other users or their comments/posts and should inform the audience exactly why the action was taken
* If you feel that you or someone else is subject to abuse by colleagues through use of a social networking site, then this action must be reported using the agreed school protocols.

### Tone

The tone of content published on social media should be appropriate to the audience, whilst retaining appropriate levels of professional standards. Key words to consider when composing messages are:

* Engaging
* Conversational
* Informative
* Friendly (on certain platforms, e.g. Facebook)

## Use of Images

School use of images can be assumed to be acceptable, providing the following guidelines are strictly adhered to.

* **Permission to use any photos or video recordings should be sought in line with the schools digital and video images policy.** If anyone, for any reason, asks not to be filmed or photographed then their wishes should be respected.
* **Under no circumstances should staff share or upload student/pupil pictures online other than via school owned social media accounts**
* Staff should exercise their professional judgement about whether an image is appropriate to share on school social media accounts. Students/pupils should be appropriately dressed, not be subject to ridicule and must not be on any school list of children whose images must not be published.
* If a member of staff inadvertently takes a compromising picture which could be misconstrued or misused, they must delete it immediately.

## Personal Use

* **Staff**
	+ Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.
	+ Personal communications which do not refer to or impact upon the school are outside the scope of this policy.
	+ Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
	+ The school permits reasonable and appropriate access to private social media sites.
* **Pupil/Students**
	+ **Staff are not permitted to follow or engage with current or prior pupils/students of the school on any personal social media network account.**
	+ The schools’ education programme should enable the pupils/students to be safe and responsible users of social media.
	+ Pupils/students are encouraged to comment or post appropriately about the school. Any offensive or inappropriate comments will be resolved by the use of the schools’ behaviour policy
* **Parents/Carers**
	+ **If parents/carers have access to a school learning platform where posting or commenting is enabled, parents/carers will be informed about acceptable use.**
	+ The school has an active parent/carer education programme which supports the safe and positive use of social media. This includes information on the website.
	+ Parents/Carers are encouraged to comment or post appropriately about the school. In the event of any offensive or inappropriate comments being made, the school will ask the parent/carer to remove the post and invite them to discuss the issues in person. If necessary, refer parents to the schools’ complaints procedures.

## Monitoring Posts About the School

* As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school.
* The school should effectively respond to social media comments made by others according to a defined policy or process.

## Appendix

### Managing your Personal Use of Social Media

* “Nothing” on social media is truly private
* Social media can blur the lines between your professional and private life. Don’t use the school logo and/or branding on personal accounts
* Check your settings regularly and test your privacy
* Keep an eye on your digital footprint
* Keep your personal information private
* Regularly review your connections – keep them to those you want to be connected to
* When posting online consider; Scale, Audience and Permanency of what you post
* If you want to criticise, do it politely.
* Take control of your images – do you want to be tagged in an image? What would children or parents say about you if they could see your images?
* Know how to report a problem

## Managing School Social Media Accounts

### The Do’s

* Check with a senior leader before publishing content that may have controversial implications for the school
* Use a disclaimer when expressing personal views
* Make it clear who is posting content
* Use an appropriate and professional tone
* Be respectful to all parties
* Ensure you have permission to ‘share’ other peoples’ materials and acknowledge the author
* Express opinions but do so in a balanced and measured manner
* Think before responding to comments and, when in doubt, get a second opinion
* Seek advice and report any mistakes using the school’s reporting process
* Consider turning off tagging people in images where possible

### The Don’ts

* Don’t make comments, post content or link to materials that will bring the school into disrepute
* Don’t publish confidential or commercially sensitive material
* Don’t breach copyright, data protection or other relevant legislation
* Consider the appropriateness of content for any audience of school accounts, and don’t link to, embed or add potentially inappropriate content
* Don’t post derogatory, defamatory, offensive, harassing or discriminatory content
* Don’t use social media to air internal grievances

## Acknowledgements

With thanks to Rob Simmonds of Well Chuffed Comms ([wellchuffedcomms.com](http://wellchuffedcomms.com)) and Chelmsford College for allowing the use of their policies in the creation of this policy.

# School Policy Template – Online Safety Group Terms of Reference

### 1. Purpose

To provide a consultative group that has wide representation from the [school] community, with responsibility for issues regarding online safety and the monitoring the online safety policy including the impact of initiatives. Depending on the size or structure of the school this group may be part of the safeguarding group. The group will also be responsible for regular reporting to the Full Governing Body.

### 2. Membership

1. The online safety group will seek to include representation from all stakeholders.

The composition of the group should include (N.B. in small schools one member of staff may hold more than one of these posts):

[add/delete where appropriate]
* SLT member/s
* Child Protection/Safeguarding officer
* Teaching staff member
* Support staff member
* Online safety coordinator (not ICT coordinator by default)
* Governor
* Parent/Carer
* ICT Technical Support staff (where possible)
* Community users (where appropriate)
* Student/pupil representation – for advice and feedback. Student/pupil voice is essential in the make-up of the online safety group, but students/pupils would only be expected to take part in committee meetings where deemed relevant.
1. Other people may be invited to attend the meetings at the request of the Chairperson on behalf of the committee to provide advice and assistance where necessary.
2. Committee members must declare a conflict of interest if any incidents being discussed directly involve themselves or members of their families.
3. Committee members must be aware that many issues discussed by this group could be of a sensitive or confidential nature
4. When individual members feel uncomfortable about what is being discussed they should be allowed to leave the meeting with steps being made by the other members to allow for these sensitivities

### 3. Chairperson

The Committee should select a suitable Chairperson from within the group. Their responsibilities include:

* Scheduling meetings and notifying committee members;
* Inviting other people to attend meetings when required by the committee;
* Guiding the meeting according to the agenda and time available;
* Ensuring all discussion items end with a decision, action or definite outcome;
* Making sure that notes are taken at the meetings and that these with any action points are distributed as necessary

### 4. Duration of Meetings

Meetings shall be held [insert frequency] for a period of [insert number] hour(s). A special or extraordinary meeting may be called when and if deemed necessary.

### 5. Functions

These are to assist the Online Safety Lead (or other relevant person) with the following [add/delete where relevant]:

* To keep up to date with new developments in the area of online safety
* To (at least) annually review and develop the online safety policy in line with new technologies and incidents
* To monitor the delivery and impact of the online safety policy
* To monitor the log of reported online safety incidents (anonymous) to inform future areas of teaching/learning/training.
* To co-ordinate consultation with the whole school community to ensure stakeholders are up to date with information, training and/or developments in the area of online safety. This could be carried out through [add/delete as relevant]:
* Staff meetings
* Student/pupil forums (for advice and feedback)
* Governors meetings
* Surveys/questionnaires for students/pupils, parents/carers and staff
* Parents evenings
* Website/VLE/Newsletters
* Online safety events
* Internet Safety Day (annually held on the second Tuesday in February)
* Other methods
* To ensure that monitoring is carried out of Internet sites used across the school
* To monitor filtering/change control logs (e.g. requests for blocking/unblocking sites).
* To monitor the safe use of data across the school
* To monitor incidents involving cyberbullying for staff and pupils

### 6. Amendments

The terms of reference shall be reviewed annually from the date of approval. They may be altered to meet the current needs of all committee members, by agreement of the majority

The above Terms of Reference for [insert name of organisation] have been agreed

Signed by (SLT):

Date:

Date for review:

## Acknowledgement

This template terms of reference document is based on one provided to schools by Somerset County Council

# Links to Other Organisations or Documents

The following links may help those who are developing or reviewing a school online safety policy and creating their online safety provision:

### UK Safer Internet Centre

Safer Internet Centre – <https://www.saferinternet.org.uk/>

South West Grid for Learning - <https://swgfl.org.uk/>

Childnet – <http://www.childnet-int.org/>

Professionals Online Safety Helpline - <http://www.saferinternet.org.uk/about/helpline>

Revenge Porn Helpline - <https://revengepornhelpline.org.uk/>

Internet Watch Foundation - <https://www.iwf.org.uk/>

Report Harmful Content - <https://reportharmfulcontent.com/>

### CEOP

CEOP - <http://ceop.police.uk/>

[ThinkUKnow](http://www.thinkuknow.co.uk/) - <https://www.thinkuknow.co.uk/>

### Others

[LGfL – Online Safety Resources](https://www.lgfl.net/online-safety/resource-centre?a=3)

[Kent – Online Safety Resources page](http://www.kelsi.org.uk/child-protection-and-safeguarding/e-safety/e-safety-classroom-materials)

INSAFE/Better Internet for Kids - <https://www.betterinternetforkids.eu/>

UK Council for Internet Safety (UKCIS) - <https://www.gov.uk/government/organisations/uk-council-for-internet-safety>

Netsmartz - <http://www.netsmartz.org/>

### Tools for Schools

Reputation Alerts – <https://swgfl.org.uk/products/reputation-alerts/>

Whisper: Anonymous Reporting Tool – <https://swgfl.org.uk/products/whisper/>

360 Degree Safe – Online Safety self-review tool – <https://360safe.org.uk/>

360Data – online data protection self-review tool: <https://360data.org.uk>

SWGfL Test filtering - <http://testfiltering.com/>

UKCIS Digital Resilience Framework - <https://www.gov.uk/government/publications/digital-resilience-framework>

### Bullying/Online-bullying/Sexting/Sexual Harrassment

Enable – European Anti Bullying programme and resources (UK coordination/participation through SWGfL & Diana Awards) - <http://enable.eun.org/>

SELMA – Hacking Hate - <https://selma.swgfl.co.uk>

Scottish Anti-Bullying Service, Respectme - <http://www.respectme.org.uk/>

Scottish Government - Better relationships, better learning, better behaviour - <http://www.scotland.gov.uk/Publications/2013/03/7388>

DfE - Cyberbullying guidance - <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyberbullying_Advice_for_Headteachers_and_School_Staff_121114.pdf>

Childnet – Cyberbullying guidance and practical PSHE toolkit:

<http://www.childnet.com/our-projects/cyberbullying-guidance-and-practical-toolkit>

[Childnet – Project deSHAME – Online Sexual Harrassment](http://www.childnet.com/our-projects/project-deshame)

[UKSIC – Sexting Resources](https://www.saferinternet.org.uk/advice-centre/teachers-and-professionals/teaching-resources/sexting-resources)

Anti-Bullying Network – <http://www.antibullying.net/cyberbullying1.htm>

[Ditch the Label – Online Bullying Charity](https://www.ditchthelabel.org/)

[Diana Award – Anti-Bullying Campaign](http://www.antibullyingpro.com/)

### Social Networking

Digizen – [Social Networking](http://digizen.org/socialnetworking/)

UKSIC - [Safety Features on Social Networks](http://www.saferinternet.org.uk/advice-and-resources/teachers-and-professionals/safety-features)

[Children’s Commissioner, TES and Schillings – Young peoples’ rights on social media](https://www.tes.com/teaching-resources/digital-citizenship)

### Curriculum

53

SWGfL Evolve - <https://projectevolve.co.uk>

[UKCCIS – Education for a connected world framework](https://www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis)

Teach Today – [www.teachtoday.eu/](http://www.teachtoday.de/en/)

Insafe - [Education Resources](http://lreforschools.eun.org/web/guest/insafe)

### Data Protection

[360data - free questionnaire and data protection self review tool](http://360data.org.uk/)

[ICO Guides for Education (wide range of sector specific guides)](https://ico.org.uk/for-organisations/education/)

[DfE advice on Cloud software services and the Data Protection Act](https://www.gov.uk/government/publications/cloud-software-services-and-the-data-protection-act)

[IRMS - Records Management Toolkit for Schools](https://c.ymcdn.com/sites/irms.site-ym.com/resource/collection/8BCEF755-0353-4F66-9877-CCDA4BFEEAC4/2016_IRMS_Toolkit_for_Schools_v5_Master.pdf)

[NHS - Caldicott Principles (information that must be released)](https://www.igt.hscic.gov.uk/Caldicott2Principles.aspx)

[ICO Guidance on taking photos in schools](https://ico.org.uk/for-the-public/schools/photos/)

[Dotkumo - Best practice guide to using photos](http://campuspr.co.uk/wp-content/uploads/2017/10/Commissioning-original-photography.pdf)

### Professional Standards/Staff Training

[DfE – Keeping Children Safe in Education](https://www.gov.uk/government/publications/keeping-children-safe-in-education--2)

DfE - [Safer Working Practice for Adults who Work with Children and Young People](http://www.safeguardinginschools.co.uk/wp-content/uploads/2015/10/Guidance-for-Safer-Working-Practices-2015-final1.pdf%22%20%5Ct%20%22_blank)

[Childnet – School Pack for Online Safety Awareness](http://www.childnet.com/resources/school-pack-for-online-safety-awareness)

[UK Safer Internet Centre Professionals Online Safety Helpline](http://www.saferinternet.org.uk/helpline)

### Infrastructure/Technical Support

[UKSIC – Appropriate Filtering and Monitoring](https://www.saferinternet.org.uk/advice-centre/teachers-and-school-staff/appropriate-filtering-and-monitoring)

SWGfL Safety & [Security](https://swgfl.org.uk/resources/) Resources

Somerset - [Questions for Technical Support](https://www.somerset.org.uk/sites/edtech/eSafety/Leading/Questions%20for%20Technical%20Support%202018.pdf)

NCA – [Guide to the Computer Misuse Act](https://nationalcrimeagency.gov.uk/who-we-are/publications/75-guide-to-the-computer-misuse-act/file)

NEN –  Advice and Guidance Notes

### Working with Parents and Carers

[Online Safety BOOST Presentations - parent’s presentation](http://www.swgfl.org.uk/boost)

[Vodafone Digital Parents Magazine](http://www.vodafone.com/content/parents/digital-parenting.html)

[Childnet Webpages for Parents & Carers](http://www.childnet.com/parents-and-carers)

[Get Safe Online - resources for parents](http://www.getsafeonline.org/nqcontent.cfm?a_id=1182)

[Teach Today - resources for parents workshops/education](http://www.teachtoday.de/en/%22%20%5Ct%20%22_blank)

[Internet Matters](https://www.internetmatters.org/)

### Prevent

[Prevent Duty Guidance](https://www.gov.uk/government/publications/prevent-duty-guidance)

[Prevent for schools – teaching resources](http://www.preventforschools.org/)

[NCA – Cyber Prevent](https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime/cyber-crime-preventing-young-people-from-getting-involved)

[Childnet - Trust Me](https://www.childnet.com/resources/trust-me)

### Research

Ofcom –Media Literacy Research

Further links can be found at the end of the UKCIS [Education for a Connected World Framework](https://www.gov.uk/government/publications/education-for-a-connected-world)

# Glossary of Terms

**AUP/AUA** Acceptable Use Policy/Agreement – see templates earlier in this document

**CEOP** Child Exploitation and Online Protection Centre (part of National Crime Agency, UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes.

**CPD** Continuous Professional Development

**FOSI** Family Online Safety Institute

**ICO** Information Commissioners Office

**ICT** Information and Communications Technology

**INSET** In Service Education and Training

**IP address** The label that identifies each computer to other computers using the IP (internet protocol)

**ISP** Internet Service Provider

**ISPA** Internet Service Providers’ Association

**IWF** Internet Watch Foundation

**LA** Local Authority

**LAN** Local Area Network

**MAT** Multi Academy Trust

**MIS** Management Information System

**NEN** National Education Network – works with the Regional Broadband Consortia (e.g. SWGfL) to provide the safe broadband provision to schools across Britain.

55

**Ofcom** Office of Communications (Independent communications sector regulator)

**SWGfL** South West Grid for Learning Trust – the Regional Broadband Consortium of SW Local Authorities – is the provider of broadband and other services for schools and other organisations in the SW

**TUK** Think U Know – educational online safety programmes for schools, young people and parents.

**UKSIC** UK Safer Internet Centre – EU funded centre. Main partners are SWGfL, Childnet and Internet Watch Foundation.

**UKCIS** UK Council for Internet Safety

**VLE** Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting,

**WAP** Wireless Application Protocol

56

54

57

A more comprehensive glossary can be found at the end of the UKCIS [Education for a Connected World Framework](https://www.gov.uk/government/publications/education-for-a-connected-world)

# Copyright & Disclaimer

Copyright of the SWGfL School Online Safety Policy Templates is held by SWGfL. Schools and other educational institutions who purchased this resource are permitted use of the templates. Any person or organisation wishing to use this resource should seek consent from SWGfL and acknowledge its use.

Every reasonable effort has been made to ensure that the information included in this template is accurate, as at the date of publication in December 2019. However, SWGfL cannot guarantee its accuracy, nor can it accept liability in respect of the use of the material whether in whole or in part and whether modified or not. Suitable legal/professional advice should be sought if any difficulty arises in respect of any aspect of this new legislation or generally to do with school conduct or discipline.

1. Authorised device – purchased by the pupil/family through a school-organised scheme. This device may be given full access to the network as if it were owned by the school [↑](#footnote-ref-1)
2. The school should add below any specific requirements about the use of personal devices in the school e.g. storing in a secure location, use during the day, liability, taking images etc. [↑](#footnote-ref-2)