# **Appendix C3 from Online Safety Policy Templates**

4

# **C3 School Online Safety Policy Template: Electronic Devices - Searching Screening and Confiscation (updated with new DfE guidance – September 2022)**

[**The DfE guidance – Searching, Screening and Confiscation**](https://www.gov.uk/government/publications/searching-screening-and-confiscation) **was updated in July 2022.**

**Please note this guidance pertains only to schools in England.**

The Education Act 2012, the basis of this template, sets out what the law is presumed to be, based on prior legal and educational knowledge, and common sense. Rights and responsibilities regarding physical contact and personal data are still evolving rapidly. So too are social, entertainment and educational technologies and the skills necessary to use them safely and prudently. This is particularly so where those who are under 18 are involved.

No existing law or policy can fully insulate anyone from the risk involved in searching for, access to or deletion of the personal data of others. Anyone refraining from any such search, access or deletion when hindsight shows circumstances merit such actions may however be at significant risk and may put seriously at risk the wellbeing of children entrusted to their care. This template cannot therefore be relied on as justification for any act or lack of action by anyone – there is no substitute for the proper and well documented exercise of adequately informed professional judgement.

It is for each school’s Headteacher and Governors/Trustees to set, apply and monitor application of their own policies as guided by their head teacher, local authority and official guidance, especially if the school is local authority maintained. This template is intended as an aide to this. South West Grid for Learning Trust does not and cannot accept and does not have responsibility for any school’s policy on this or any other matter.

Within this template, sections which include information or guidance are shown in BLUE. It is anticipated that schools will remove these sections from their completed policy documents, though this will be for the school’s relevant policy advisory group to recommend and for the head teacher and other governors to decide upon.

*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 ought to be an essential part of a school online safety policy.**

The template uses the term learners to refer to the children/young people attending the learning institution and the term Headteacher to refer to Headteachers or Principals, as relevant.

### Introduction

The changing face of information technologies and ever-increasing learner use of these technologies has meant that the Education Acts were updated to keep pace. Part 2 of the Education Act 2011 (Discipline) introduced changes to the powers afforded to schools by statute to search learners in order to maintain discipline and ensure safety. Schools are required to ensure they have updated policies which take these changes into account. No such policy can on its own guarantee that the school will not face legal challenge but having a robust policy which takes account of the Act and applying it in practice will however help to provide the school with justification for what it does.

The particular changes we deal with here are the added power to screen, confiscate and search for items ‘banned under the school rules’ and the power to ‘delete data’ stored on confiscated electronic devices.

Items banned under the school rules are determined and publicised by the Headteacher (section 89 Education and Inspections Act 1996).

An item banned by the school rules may only be searched for under these new powers if it has been identified in the school rules as an item that can be searched for. It is therefore important that there is a school policy which sets out clearly and unambiguously the items which:

* are banned under the school rules; and
* are banned AND can be searched for by authorised school staff

The act allows authorised persons to examine data on electronic devices if they think there is a good reason to do so. In determining a ‘good reason’ to examine or erase the data or files the authorised staff member must reasonably suspect that the data or file on the device in question relates to an offence and/or may be used to cause harm, to disrupt teaching or could break the school rules.

Following an examination, if the person has decided to return the device to the owner, or to retain or dispose of it, they may erase any data or files, **if they think there is a good reason to do so** (see later section)

The Headteacher must publicise the school behaviour policy, in writing, to staff, parents/carers and learners at least once a year. (There should therefore be clear links between the search etc. policy and the behaviour policy).

DfE advice on these sections of the Education Act 2011 can be found in the document[: “Screening, searching and confiscation – Advice for schools”](https://www.gov.uk/government/publications/searching-screening-and-confiscation) (**updated July 2022**)

It is recommended that Headteachers (and, at the least, one other senior leader) should be familiar with this guidance.

**The DfE Guidance – “**[**Behaviour in Schools**](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1089687/Behaviour_in_Schools_guidance_July_2022.pdf)**” was updated in July 2022 and refers to behaviour online:**

“The way in which pupils relate to one another online can have a significant impact on the culture at school. Negative interactions online can damage the school’s culture and can lead to school feeling like an unsafe place. Behaviour issues online can be very difficult to manage given issues of anonymity, and online incidents occur both on and off the school premises. Schools should be clear that even though the online space differs in many ways, the same standards of behaviour are expected online as apply offline, and that everyone should be treated with kindness, respect and dignity.

Inappropriate online behaviour including bullying, the use of inappropriate language, the soliciting and sharing of nude or semi-nude images and videos and sexual harassment should be addressed in accordance with the same principles as offline behaviour, including following the child protection policy and speaking to the designated safeguarding lead (or deputy) when an incident raises a safeguarding concern.

Many online behaviour incidents amongst young people occur outside the school day and off the school premises. Parents are responsible for this behaviour. However, often incidents that occur online will affect the school culture. Schools should have the confidence to sanction pupils when their behaviour online poses a threat or causes harm to another pupil, and/or could have repercussions for the orderly running of the school, when the pupil is identifiable as a member of the school or if the behaviour could adversely affect the reputation of the school.

Headteachers should decide if **mobile phones** can be used during the school day. Many pupils, especially as they get older, will have one of their own. Allowing access to mobiles in school introduces complexity and risks, including distraction, disruption, bullying and abuse, and can be a detriment to learning. Headteachers should consider restricting or prohibiting mobile phones to reduce these risks.

If headteachers decide not to impose any restrictions on mobile phones, they should have a clear plan to mitigate the risks of allowing access to phones. This plan, as part of the school’s behaviour policy, should outline the approach to mobile phones and be reiterated to all pupils, staff and parents throughout the school year. Headteachers should ensure it is consistently and fairly applied.”

**A new** [**Keeping Children Safe in Education**](https://www.gov.uk/government/publications/keeping-children-safe-in-education--2) **guidance document is in force from September 2022.** Schools should be aware of new guidance concerning **Harmful Sexual Behaviour** (see policy template in these appendices):

“Following any report of child-on-child sexual violence or sexual harassment offline or online, schools should follow the general safeguarding principles set out in Keeping children safe in education (KCSIE) - especially Part 5. The designated safeguarding lead (or deputy) is the most appropriate person to advise on the school’s initial response. Each incident should be considered on a case-by-case basis.

Schools should be clear in every aspect of their culture that sexual violence and sexual harassment are never acceptable, will not be tolerated and that pupils whose behaviour falls below expectations will be sanctioned. Schools should make clear to all staff the importance of challenging all inappropriate language and behaviour between pupils. Schools should refer to the Respectful School Communities toolkit for advice on creating a culture in which sexual harassment of all kinds is treated as unacceptable.”

### Relevant legislation:

* Education Act 1996
* Education and Inspections Act 2006
* Education Act 2011 Part 2 (Discipline)
* The School Behaviour (Determination and Publicising of Measures in Academies) Regulations 2012
* Health and Safety at Work etc. Act 1974
* Obscene Publications Act 1959
* Children Act 1989
* Human Rights Act 1998
* Computer Misuse Act 1990

This is not a full list of Acts involved in the formation of this advice. Further information about relevant legislation can be found via the above link to the DfE advice document.

### Responsibilities

The Headteacher is responsible for ensuring that the school policies reflect the requirements contained within the relevant legislation. The formulation of these policies may be delegated to other individuals or groups. The policies will normally be taken to Governors for approval. The Headteacher will need to authorise those staff who are allowed to carry out searches.

This policy has been written by and will be reviewed by: insert relevant names/roles/group

The Headteacher has authorised the following members of staff to carry out searches for and of electronic devices and the deletion of data/files on those devices: (the policy should here list those staff/roles given such authority. A Headteacher may choose to authorise all staff willing to be authorised, but should consider training needs in making this decision).

The Headteacher may authorise other staff members in writing in advance of any search they may undertake, subject to appropriate training.

Members of staff (other than Security Staff) cannot be required to carry out such searches. They can each choose whether or not they wish to be an authorised member of staff.

### Training/Awareness

It is essential that all staff should be made aware of and should implement the school’s policy.

Members of staff should be made aware of the school’s policy on "Electronic devices – searching, confiscation and deletion":

* at induction
* at regular updating sessions on the school’s online safety policy

Members of staff authorised by the Headteacher to carry out searches for and of electronic devices and to access and delete data/files from those devices should receive training that is specific and relevant to this role.

Specific training is required for those staff who may need to judge whether material that is accessed is inappropriate or illegal.

35

### Policy Statements

## Screening

DfE  [“Screening, searching and confiscation – Advice for schools”](https://www.gov.uk/government/publications/searching-screening-and-confiscation) allows schools to use screening:

“Screening can help provide reassurance to pupils, staff and parents that the school is taking measures to create a calm, safe and supportive environment.

Schools’ statutory power to make rules on pupil behaviour and their duties as employers in relation to the safety of staff, pupils and visitors enables them to impose a requirement that pupils undergo screening.

Screening is the use of a walk-through or hand-held metal detector (arch or wand) to scan all pupils for weapons before they enter the school premises..

If a headteacher decides to introduce a screening arrangement, they should inform pupils and parents in advance to explain what the screening will involve and why it will be introduced.”

The school should add here details of any screening arrangements that are in place:

#### Search:

The school **Behaviour Policy** refers to the policy regarding searches with and without consent for the wide range of items covered within the Education Act 2011 and lists those items. This policy refers only to the searching for and of electronic devices and the deletion of data/files on those devices.

The school will already have a policy relating to whether or not mobile phones and other electronic devices are banned, or are allowed only within certain conditions. The school should therefore consider including one of the following statements in the policy:

**Either:**

*Learners are not allowed to bring mobile phones or other personal electronic devices to school or use them in the school.*

**Or**

*Learners are allowed to bring mobile phones or other personal electronic devices to school and use them only within the rules laid down by the school.* (you should refer to the relevant policy or to list here the conditions under which they are allowed)

If learners breach these roles:

**Either:**

*The sanctions for breaking these rules will be:* (list here)

**Or**

*The sanctions for breaking these rules can be found in the* (name the policy - for most schools this will be the Behaviour Policy)

Authorised staff (defined in the responsibilities section above) have the right to search for such electronic devices where they reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the school rules.

* Searching with consent - Authorised staff may search with the learner’s consent for any item
* Searching without consent - Authorised staff may only search without the learner’s consent for anything which is either ‘prohibited’ (as defined in Section 550AA of the Education Act 1996) or appears in the school rules as an item which is banned and may be searched for

#### In carrying out the search:

The authorised member of staff must have reasonable grounds for suspecting that a *learner* is in possession of a prohibited item i.e. an item banned by the school rules and which can be searched for. (Whether there are ‘reasonable grounds’ is a matter decided on by reference to the circumstances witnessed by, or reported to, someone who is authorised and who exercises properly informed professional judgment and has received appropriate training).

The authorised member of staff should take reasonable steps to check the ownership of the mobile phone/personal electronic device before carrying out a search. (The powers included in the Education Act do not extend to devices owned (or mislaid) by other parties e.g. a visiting parent or contractor, only to devices in the possession of learners.)

The authorised member of staff should take care that, where possible, searches should not take place in public places e.g. an occupied classroom, which might be considered as exploiting the learner being searched.

The authorised member of staff carrying out the search must be the same gender as the *learner* being searched; and there must be a witness (also a staff member) and, if at all possible, they too should be the same gender as the *learner* being searched.

There is a limited exception to this rule: Authorised staff can carry out a search of a learner of the opposite gender including without a witness present, but **only where you reasonably believe that there is a risk that serious harm will be caused to a person if you do not conduct the search immediately and where it is not reasonably practicable to summon another member of staff.**

#### Extent of the search:

**The person conducting the search may not require the learner to remove any clothing other than outer clothing.**

Outer clothing means clothing that is not worn next to the skin or immediately over a garment that is being worn as underwear (outer clothing includes hats; shoes; boots; coat; blazer; jacket; gloves and scarves).

‘Possessions’ means any goods over which the learner has or appears to have control – this includes desks, lockers and bags. (schools will need to take account of their normal policies regarding religious garments/headwear and may wish to refer to it in this policy)

*A* learner’s possessions can only be searched in the presence of the learner and another member of staff, except where there is a risk that serious harm will be caused to a person if the search is not conducted immediately and where it is not reasonably practicable to summon another member of staff.

**The power to search without consent enables a personal search, involving removal of outer clothing and searching of pockets; but not an intimate search going further than that, which only a person with more extensive powers (e.g. a police officer) can do.**

**Use of Force – force cannot be used to search without consent for items banned under the school rules regardless of whether the rules say an item can be searched for.**

### 

### Electronic devices

[The DfE guidance – Searching, Screening and Confiscation](https://www.gov.uk/government/publications/searching-screening-and-confiscation)received significant updates in July 2022 and now states:

* Electronic devices, including mobile phones, can contain files or data which relate to an offence, or which may cause harm to another person. This includes, but is not limited to, indecent images of children, pornography, abusive messages, images or videos, or evidence relating to suspected criminal behaviour.
* As with all prohibited items, staff should first consider the appropriate safeguarding response if they find images, data or files on an electronic device that they reasonably suspect are likely to put a person at risk
* Staff may examine any data or files on an electronic device they have confiscated as a result of a search .. if there is good reason to do so (defined earlier in the guidance as)
  + poses a risk to staff or pupils;
  + is prohibited, or identified in the school rules for which a search can be made or
  + is evidence in relation to an offence.
* If the member of staff conducting the search suspects they may find an indecent image of a child (sometimes known as nude or semi-nude images), the member of staff should never intentionally view the image, and must never copy, print, share, store or save such images. When an incident might involve an indecent image of a child and/or video, the member of staff should confiscate the device, avoid looking at the device and refer the incident to the designated safeguarding lead (or deputy) as the most appropriate person to advise on the school’s response. Handling such reports or concerns can be especially complicated and schools should follow the principles as set out in [Keeping children safe in education](https://www.gov.uk/government/publications/keeping-children-safe-in-education--2). The UK Council for Internet Safety also provides the following guidance to support school staff and designated safeguarding leads: [Sharing nudes and semi-nudes: advice for education settings working with children and young people.](https://www.gov.uk/government/publications/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people/sharing-nudes-and-semi-nudes-how-to-respond-to-an-incident-overview)
* If a member of staff finds any image, data or file that they suspect might constitute a specified offence, then they must be delivered to the police as soon as is reasonably practicable.
* In exceptional circumstances members of staff may dispose of the image or data if there is a good reason to do so. In determining a ‘good reason’ to examine or erase the data or files, the member of staff must have regard to the following guidance issued by the Secretary of State
  + In determining whether there is a ‘good reason’ to examine the data or files, the member of staff should reasonably suspect that the data or file on the device has been, or could be used, to cause harm, undermine the safe environment of the school and disrupt teaching, or be used to commit an offence.
  + In determining whether there is a ‘good reason’ to erase any data or files from the device, the member of staff should consider whether the material found may constitute evidence relating to a suspected offence. In those instances, the data or files should not be deleted, and the device must be handed to the police as soon as it is reasonably practicable. If the data or files are not suspected to be evidence in relation to an offence, a member of staff may delete the data or files if the continued existence of the data or file is likely to continue to cause harm to any person and the pupil and/or the parent refuses to delete the data or files themselves

The examination of the data/files on the device should go only as far as is reasonably necessary to establish the facts of the incident. Any further intrusive examination of personal data may leave the school open to legal challenge. It is important that authorised staff should have training and sufficient knowledge of electronic devices and data storage.

Members of staff may require support in judging whether the material is inappropriate or illegal. One or more Senior Leaders should receive additional training to assist with these decisions. Care should be taken not to delete material that might be required in a potential criminal investigation.

The school should also consider their duty of care responsibility in relation to those staff who may access disturbing images or other inappropriate material whilst undertaking a search. Seeing such material can be most upsetting. There should be arrangements in place to support such staff. The school may wish to add further detail about these arrangements.

Further guidance on reporting the incident to the police and the preservation of evidence can be found in the SWGfL flow chart in the main School Template Policies document. Local authorities/local safeguarding partnerships may also have further guidance, specific to their area.

A record should be kept of the reasons for the deletion of data/files. (DfE guidance states and other legal advice recommends that there is no legal reason to do this, best practice suggests that the school can refer to relevant documentation created at the time of any search or data deletion in the event of a learner, parental or other interested party complaint or legal challenge. Records will also help the school to review online safety incidents, learn from what has happened and adapt and report on application of policies as necessary).

### Care of Confiscated Devices

School staff are reminded of the need to ensure the safe keeping of confiscated devices, to avoid the risk of compensation claims for damage/loss of such devices (particularly given the possible high value of some of these devices).

The school may wish to add a disclaimer to the relevant section of the Behaviour Policy which may assist in covering the school against damage/loss claims.

### Audit/Monitoring/Reporting/Review

The responsible person (insert title) will ensure that full records are kept of incidents involving the searching for and of electronic devices and the deletion of data/files. (a template log sheet can be found in the appendices to the School Online Safety Template Policies)

These records will be reviewed by ... (*Online Safety Officer/Online Safety Committee/Online Safety Governor*) at regular intervals (state the frequency).

This policy will be reviewed by the head teacher and governors annually and in response to changes in guidance and evidence gained from the records.

The school is required is publish its Behaviour Policy to parents annually (including on its website) – the Behaviour Policy should be cross referenced with this policy on search and deletion. DfE guidance can be found at: <https://www.gov.uk/government/publications/searching-screening-and-confiscation>

Copyright of these policy templates is held by SWGfL. Schools/colleges and other educational institutions are permitted free use of the policy templates for the purposes of policy review and development. Any person or organisation wishing to use the document for other purposes should seek consent from SWGfL ([onlinesafety@swgfl.org.uk](mailto:onlinesafety@swgfl.org.uk)) and acknowledge its use.

Every effort has been made to ensure that the information included in this document is accurate, as at the date of publication in September 2022. However, SWGfL cannot guarantee its accuracy, nor can it accept liability in respect of the use of the material.

© SWGfL 2022