Pendle
Education Trust

Castercliff Primary Academy

Electronic Searching and Deletion Policy

Author of Policy:	Kirsty Johnson
Policy Approved By:	Mark Sherwin
Date:	March 2024
Review date:	March 2025

Pendle Education Trust
Nelson and Colne College, Scotland Road, Nelson, BB9 7YT
Tel 01282 440 249 Email contact@pendleeducationtrust.co.uk
Company Registration Number: 08263591
Place of Registration: England and Wales

Introduction:

The changing face of information technologies and ever increasing pupil use of these technologies has meant that the Education Acts have had to change in an attempt to keep pace. Within Part 2 of the Education Act 2011 (Discipline) there have been changes to the powers afforded to schools by statute to search pupils 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 search for items 'banned under the school rules' and the power to 'delete data' stored on seized electronic devices.

Items banned under the school rules are determined and publicised by the Principal (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 has been, or could 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 doso.

The Principal must publicise the school behaviour policy, in writing, to staff, parents / carers and pupils at least once a year.

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) Regulations2012
- Health and Safety at Work etc. Act 1974
- Obscene Publications Act 1959
- Children Act 1989
- Human Rights Act 1998

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 DfE advice can be found in the document: "Screening, searching and confiscation – Advice for head teachers, staff and governing bodies"

http://www.education.gov.uk/schools/pupilsupport/behaviour/behaviourpolicies/f0076897/screening- searching-and-confiscation

Responsibilities

The Principal and Online Safety Leader will need to ensure that the school behaviour policy (in the case of devices in the possession of pupils), Staff and Visitor Acceptable Use Policies (in the case of devices in the possession of staff and visitors) and Parental Consent (in the case of devices in the possession of parents/carers) reflect the requirements contained within the relevant legislation and authorise those staff who are allowed to carry out searches.

The Principal has authorised all academy DSLs to carry out searches for and of electronic devices and the deletion of data / files on those devices. At least two members of authorised staff must be present at any search / deletion of data and the incident recorded on CPOMS.

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

Training / Awareness

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

- at induction
- at regular updating sessions on the school's Online Safety policy

Members of staff authorised by the Principal 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.

Policy Statements:

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 (when found in the possession of pupils). This policy refers only to the searching for and of electronic devices and the deletion of data / files on those devices.

Pupils are not allowed to bring mobile phones or other personal electronic devices to school or use them in the school. The sanctions for breaking these rules can be found in the Behaviour Policy.

Staff and visitors are allowed to bring personal electronic devices to school, although these should remain switched off and out of sight unless an Acceptable Use Policy (see Online Safety policy) has been read and signed. Staff and visitors must adhere to strict restrictions of the use of personal electronic devices as described in the relevant Acceptable Use Policy. This policy refers to the searching for and of electronic devices and the deletion of data / files on those devices should there be concerns regarding inappropriate use of these devices.

Parents may use personal electronic devices in school in particular circumstances. All parents have signed a Parental Consent form (see Online Safety policy) outlining their responsibilities for appropriate use and sharing of images taken in school. This policy refers

to the searching for and of electronic devices and the deletion of data / files on those devices should there be concerns regarding inappropriate use of these devices.

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, disrupt teaching or break the school rules / terms of an agreed Acceptable Use Policy.

Search (Pupils Only):

- Searching with consent - Authorised staff may search with the pupil's consent for any item.
- Searching without consent - Authorised staff may search without the pupil's consent for anything which is either 'prohibited' (as defined in Section 550AA of the Education Act 1996) or appears in the school behaviour policy 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 pupil 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 pupils / students.)

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 pupil being searched.

The authorised member of staff carrying out the search must be the same gender as the pupil 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 pupil being searched if possible.

There is a limited exception to this rule: Authorised staff can carry out a search of a pupil 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 pupil 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).

A pupil's possessions can only be searched in the presence of the pupil 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.

'Possessions' means any goods over which the pupil has or appears to have control – this includes all bags, lunchboxes and trays.

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.

Search (adults):

The authorised member of staff must have reasonable grounds for suspecting that an adult (staff member, visitor or parent) has used an electronic device in a way that contravenes the agreed terms of the Acceptable Use Policies (for staff and visitors) or Parental Consent (for parents) before requesting to examine an electronic device in the possession of an adult.

Electronic Devices:

An authorised member of staff finding an electronic device may access and examine any data or files on the device if they think there is a good reason to do so (i.e. the staff member must 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 / the agreed terms of an Acceptable Use Policy). Accessing an electronic device found in the possession of a pupil should be done in the presence of a parent or carer where possible.

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.

If inappropriate material is found on the device it is up to the authorised member of staff to decide whether they should delete that material, retain it as evidence (of a criminal offence or a breach of school discipline) or whether the material is of such seriousness that it requires the involvement of the police. Examples of illegal activity would include:

- child sexual abuse images (including images of one child held by another child)
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

Members of staff may require support in judging whether the material is inappropriate or illegal. Care should be taken not to delete material that might be required in a potential criminal investigation.

Castercliff Primary Academy will 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. Arrangements will be made to support such staff, in the first instance via Place2Be.

Further guidance on reporting the incident to the police and the preservation of evidence can be found in the flow chart in the 'Illegal Incidents' section of this policy.

Deletion of Data:

Following an examination of an electronic device, if the authorised member of staff 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 (i.e. the staff member must 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 / the agreed terms of an Acceptable Use Policy).

If inappropriate material is found on the device, it is up to the authorised member of staff to decide whether they should delete that material, retain it as evidence (of a possible criminal offence or a breach of school discipline) or whether the material is of such seriousness that it requires the involvement of the police.

A record should be kept of the reasons for the deletion of data / files on CPOMS. (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 pupil/student, 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 ConfiscatedDevices

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. Confiscated devices must be kept at the school office in a lockable cupboard or the in the school safe.

Audit / Monitoring / Reporting / Review

The Online Safety leader will ensure that full records are kept of incidents involving the searching for and of mobile phones and electronic devices and the deletion of data / files using CPOMS.

These records will be reviewed by the Online Safety Group at each termly meeting.

Pendle
Education Trust

Pendle Education Trust
Nelson and Colne College, Scotland Road, Nelson, BB9 7YT
Tel 01282 440 249 Email contact@pendleeducationtrust.co.uk
Company Registration Number: 08263591
Place of Registration: England and Wales