



# Search & Deletion Policy

---

## Key Document Details

|              |  |                      |               |
|--------------|--|----------------------|---------------|
| School Name: | The White Horse Federation – all schools | Ratified date:       | December 2019 |
| Version no:  | 1  | Interim review date: | n/a           |
| Author:      | J Summerson & L Newbury                  | Next review date:    | December 2020 |
| Owner:       | M Weller                                 |                      |               |
| Approved by: | CEO                                      |                      |               |

## Introduction

The Education Act 2012, 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 guidance 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 academy's Headteacher / Principal and CEO/ Trustees to set, apply and monitor the application of their own policies as guided by official guidance. This guidance is intended as an aide to this.

## Context

The changing face of information technologies and ever increasing pupil / student 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, which can be found at <http://www.legislation.gov.uk/ukpga/2011/21/part/2/enacted>

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.

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 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 do so.

The Head Teacher / Principal must publicise the school behaviour policy, in writing, to staff, parents / carers and students / pupils 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 head teachers, staff and governing bodies" (2014 and updated January 2018)

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

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

- 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

The CEO/Trustees are 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. At the local level, the Principal will need to authorise those staff who are allowed to carry out searches, and will be responsible for managing policy implementation.

The Principal shall act as the authorised member of staff in order to carry out searches for and of electronic devices and the deletion of data / files on those devices:

The Headteacher / Principal 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.

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 and deletion":

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

Members of staff authorised by the Headteacher / 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.

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

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

### Consent/Non Consensual searches

- **Searching with consent** - Authorised staff may search with the pupil's consent for any item
- **Searching without consent** - Authorised staff may only 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 rules as an item which is banned and may be searched for.

The authorised member of staff must have reasonable grounds for suspecting that a student / 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. Reasonable grounds for searching could include, but are not limited to:

- Other pupils talking about the item or
- A pupil behaving in a suspicious manner.
- The school can rely on CCTV footage to help reach their decision.

These powers apply regardless of whether any prohibited item is found on the pupil.

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 eg 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 student / pupil being searched.

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

**There is a limited exception to this rule:** Authorised staff can carry out a search of a student / 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.

The person conducting the search must not require the student/ 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).

'Possessions' means any goods over which the student / pupil has or appears to have control – this includes desks, lockers and bags.

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

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.**

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 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. 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 Online Safety Incident Reporting Flow Chart.

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). 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. Although 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).

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 Principal 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.

DfE guidance can be found at: <https://www.gov.uk/government/publications/searching-screening-and-confiscation>