Dunottar School

Electronic Devices Policy- Searches and Deletion

Contents

Electronic Devices Policy – Searching & Deletion

Policy Statement

The Education Act 2012, the basis of this policy, 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.

This policy applies to all members of the school community.

This policy is reviewed at least annually by the school senior management who will report to the Local Governing Body on its implementation on a regular (annual) basis. The date of the next review is Nov 2018.

In accordance with the school's Provision of Information Policy, the policy is made available on the school's website and in hard copy, on request, from the Main School Office. It should be read in conjunction with:

- Behaviour and Discipline Policy
- Anti-Bullying Policy
- Exclusion, Expulsion, Removal and Review Policy
- Other Technology Policies including Information Technology Policy, E-Safety Policy, Social Media Policy, Mobile Devices Policy and Filtering Policy.

The school is committed to ensuring that the implementation of this policy is non-discriminatory, in line with the UK Equality Act (2010). Further details are available in the school's own Equal Opportunities Policy.

Introduction

The changing face of information technologies and ever increasing 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 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 Headmaster (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 Headmaster Mark Tottman must publicise the school Behaviour Policy, in writing, to staff, parents / carers and students at least once a year.

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"

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/554415/searching_screening_confiscation_advice_Sept_2016.pdf

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 Headmaster Mark Tottman 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 the LGB Governors for approval. The Headmaster will need to authorise those staff who are allowed to carry out searches.

The Headmaster Mark Tottman 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:

Marc Broughton Deputy Head (Pastoral) Pippa Smithson Deputy Head (Academic)

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

Members of 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.

This policy has been written by and will be reviewed by: T.Stevens & M.Broughton. It is reviewed annually or as and when changes or legislation require. The next review date is November 2019.

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 and deletion":

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

Members of staff authorised by the Headmaster 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.

Search

This policy refers only to the searching for and of electronic devices and the deletion of data / files on electronic devices.

Pupils / students 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 which can be found in the Mobile Digital Devices Policy in the Guidance for Pupils Section.

If students breach these roles:

The sanctions for breaking these rules can be found in the Mobile Device Policy and with reference to the Behaviour Policy and Exclusions, Expulsions and Removal 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 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- *for weapons, controlled drugs, stolen items or alcohol (for students under 18)*) 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 student / pupil is in possession of a prohibited item i.e. an item banned by the school rules and which can be searched for.

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 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 being searched.

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

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

The person conducting the search may not require the student 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 has or appears to have control – this includes desks, lockers and bags.

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

Searches of 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 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.

If inappropriate material is found on the device the staff member must 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. Senior Leaders receive additional training to assist with these decisions, Marc Broughton DSL (Deputy Head pastoral) and Pippa Smithson Deputy DSL (Deputy Head Academic) will receive the required training.

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.

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).

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.

Members of staff should contact either M. Broughton DSL (Deputy Head Pastoral) or Pippa Smithson Deputy DSL (Deputy Head Academic) with any concerns or questions regarding material they are made aware of which may need investigation.

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.

Audit / Monitoring / Reporting / Review

The responsible person Marc Broughton and Thomas Stevens (Network Manager) 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.

These records will be reviewed by E-Safety Officer Marc Broughton/ E-Safety Committee / E-Safety Governor Gary Richards at regular intervals.

Name of owner/Author:		M.Thomas/ M.Broughton
Authorised By:		R.Cole
Date Document Reviewed:	Nov 2016	M.Broughton/ S.Thorne
Date Document Updated:	Sept 2017	Change of headteacher
Date Document Reviewed:	Oct 2017	M. Broughton/S.Thorne
Date Document Updated:	Jan 2018	Change of Network Manager
Date Document Updated:	April 2018	Change of Network Manager
Date Document Reviewed:	Nov 2018	ST/MB
Next Review Date:	Nov 2019	As or when events of legislation require
Governor responsible for Policy:	Andy Porteous	

END OF DOCUMENT