United Learning
The best in everyone™

Dunottar School

IT Policies

Table of Contents

Bring Your Own Device (BYOD) Policy

Bring Your Own Device Policy Statement

Dunottar School recognises the importance and benefits of mobile digital device use with the school environment and associated school trips. In addition, the majority of students and staff, for security and practical reasons, feel the need to carry a mobile phone, and for these reasons their use is allowed in school. However, as we are a working community, we need to have regulations governing the use of Wi-Fi and 5G internet enabled devices so that incoming communications do not interrupt lessons and so that students do not use them unnecessarily and disrupt the effective operation of the school.

This Policy applies to 'standard' mobile phones as well as smart phones such as, but not limited to, iPhones, Blackberries, Android and Windows phones, and other 3G/4G/5G and Wi-Fi enabled devices such as iPads, iPods, tablets, smart watches and laptops. Use of BYOD by members of staff and students is regulated, in accordance with Group Policy and recognised professional standards of acceptable practice.

The school accepts that staff and students are permitted to bring such devices to school but their use is restricted as detailed in this policy.

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 and the E-Safety LGB representative Dan Hawker on its implementation on a regular (annual) basis. The date of the next review will be October 2023.

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, Electronic 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.

Key Personnel

Mr Thomas Stevens (Network Manager)

Mr John Weiner (Deputy Head Pastoral)

Mr Dan Hawker (LGB Member)

Key personnel providing e-safety training:

Mr James Garnett (IT Director, United Learning)

Areas of Risk

Child Protection: Students on roll become associated with the school through linked social media platforms.

Risk of radicalisation and grooming through the use of social media platforms.

Bullying: Use of mobile technology can make bullying more pervasive and difficult to monitor.

Staff Protection: Content recorded in lessons, whether overtly or covertly, on BYOD may cause distress to staff, especially when uploaded to social platforms.

Procedures

A common-sense approach should be followed regarding the use of 3G, 4G, 5G and Wi-Fi enabled devices. Teachers should always have the ability to override rules against mobile device use, where common sense prevails, although the following guidelines should be used:

Times and locations where BYOD use may be permitted

- When directed by a teacher and within the context of an academic lesson, students may be given permission to use social media.
- When directed by a teacher and within the context of an academic lesson, students may be given permission to video each other or themselves on school devices only.
- Taking photos on school trips - if students use their own devices on an informal basis to take photographs of other students whilst on school trips, they must give due consideration to the appropriateness of uploading any photographs or video to social media sites.
- Taking photographs of academic work. There are times when students will want (or need) to photograph different stages of a project, practical task or experiment. In all cases, students should seek authorisation from their teacher before using cameras to record their work.
- Under direction from a member of staff, students may use either school owned cameras or their own personal mobile device to make an appropriate record of their academic work. Staff may withdraw authorisation at any time and students should be mindful of the responsibility given in allowing use of personal devices. Any images or sections of video, which are found to contain images of students, should be deleted at the earliest opportunity.
- A student may be given authorisation to video or record specific elements of a lesson, at the sole discretion of the teacher of the lesson.

Times and locations where BYOD use is not permitted

- **3G/4G/5G or Wi-Fi enabled devices of any description, including mobile phones, iPods or iPads, must never be taken into public examinations by students.**

- BYOD should be switched off or muted and in airline mode during lessons, unless directed otherwise by the member of staff in charge.
- Students should not be posting updates to social media platforms during the school day unless specifically directed to do so by a member of staff for educational purposes.
- Students should not contact their parents directly when unwell or unhappy at school, via either phone, social media or electronic methods, to arrange to be collected. The student should report to the health centre or reception who will contact their parents, if appropriate to do so. Parents should telephone the school office in the event of an emergency, and a message will be passed on in the usual way.

Guidance on safe use of BYOD

- Students should not post information about their specific location or current activity to social media platforms while on a school trip. In doing so students could affect their personal safety or that of their peers.
- In line with the school policy on use of photographs taken in school, students are not allowed to use their BYOD or cameras to take photos or videos of other students for any school purpose. It is not, for example, permissible for students to use their own devices to take videos of e.g. auditions for a school event, or a classroom activity.
- If students need to be filmed for such purposes, filming must be sanctioned by the member of staff concerned; agreed to by the student(s) concerned; and be on school devices only.
- Parents must agree to the school using its own devices to film students on occasion for internal use when their child joins the school.
- Under no circumstances should covert recording of lessons take place, or recording take place outside of the specific parameters laid out by the teacher when authorisation is given. Doing so could result in disciplinary action.
- Uploading inappropriate photos or videos could result in disciplinary action, as outlined in the Student Acceptable Use of Technology Agreement.

Sanctions for Misuse of BYOD

The school will apply appropriate sanctions to any student who uses their mobile phone, or other device, for bullying, intimidation, or for keeping, or disseminating inappropriate text or images.

Further references and information can be found in the Anti-Bullying Policy, Behaviour Policy and the Exclusions, Expulsions and Removal Policy.

The school will apply appropriate sanctions to any member of staff who uses their mobile phone, or other device, for bullying, intimidation, or for keeping, or disseminating inappropriate text or images in line with the United Learning Disciplinary Policy.

Security of Mobile Phones and other electronic devices

Students and staff are advised to have their phones/iPods/iPads or any other digital device security marked.

The school does not accept responsibility for mobile phones or other electronic communication devices or entertainment systems. Students should be advised to lock their devices in their lockers during lessons. Parents (and staff) should be informed that mobile phones and other such devices are not covered by the organisation’s insurance policy. Staff should be advised to keep valuables on them at all times, or keep them in the staffroom, though their security there cannot be guaranteed.

Cyber Bullying

Instances of cyber bullying will be punishable in accordance with the school’s Anti-Bullying Policy and may even result in exclusion or expulsion (or in disciplinary action, in the case of staff – refer to United Learning Staff Bullying and Harassment Policy).

Dealing with Inappropriate Content on BYOD

If a teacher suspects or is informed that a student has inappropriate content on their mobile device then the teacher will confiscate the device. The Deputy Head Pastoral John Weiner will investigate the matter and report to the Headmaster. During their investigations, if the student is formally interviewed, this will be with another member of staff present. A member of staff may investigate content on the mobile device in line with the Dunottar School’s Electronics Devices- Searching and Deletion Policy. The student’s parents may also be invited to attend the interview. In line with the school’s policy on Exclusion, Expulsion and Removals, the student may also be suspended whilst the allegation is being investigated. If it is discovered that the student’s mobile phone (or other electronic device) contains inappropriate images of a child or young person (under the age of 18), the Headmaster and police will be informed. The mobile device will remain in the possession of the school in a secure location with limited access until advice from the police has been acted upon.

This may include asking all students in possession of the image to delete it, if the image has been forwarded outside the school’s control contact will be made to request that third parties follow the same steps. If the image has been uploaded to any website or social networking site, contact will be made in an attempt to have it removed. The parents of all of the students involved will be notified of the situation to ensure all content on devices in the homes of the students are removed. In-house counselling will be offered to those concerned. If a formal disciplinary meeting is called, this will be in accordance with the procedure set out in the school’s Exclusion, Expulsion, and Removal Policy.

In the case of staff, any instances of inappropriate images of children or young people must be reported immediately to the Headmaster Mark Tottman and/or in the Designated Safeguarding Lead (John Weiner) or Deputy Safeguarding Leads (Nicky Jackson and Carrie Allison). The police will also be informed as well as the LADO. Information on this can be found in the Safeguarding Child Protection Policy (page 21) and further information can be found at https://www.gov.uk/government/uploads/system/uploads/attachement_data/file/551575/6.2439_KG_NCA_Sexting_in_Schools_WEB_1_.PDF

BYOD Guidelines for Pupils

1. All devices are brought into school at the pupil's own risk and the responsibility for their safekeeping lies with the pupil. The school will take no liability for loss or damage.

2. School is a place of work; pupils' mobile phones/devices must be switched off (or in silent mode) at all times whilst on school premises, unless specifically authorised by a member of staff.
3. Permission must be sought from a member of staff, and authorisation given, before a pupil may be allowed to use a mobile device on school premises.
4. If the use of a device is permitted or directed in a lesson (e.g. as a calculator, camera or voice recorder) it will be under explicit staff supervision, and permission can be withdrawn at any time.
5. Any pupil found using a device on school premises without staff permission, should ordinarily expect to have their device confiscated for the rest of the day and should collect it as instructed. They can expect to be given a detention.
6. If a pupil needs to contact home in an emergency, they must speak with a member of staff who will deal with the matter. Pupils should not contact home in the case of illness; this should only be done by a member of staff.
7. If parents need to contact pupils in an emergency, they should contact the school reception and a message will be taken to the pupil. Parents are reminded that pupils should not have their devices turned on whilst on school premises and, hence, will be unable to check for messages.
8. Pupils may only access the internet through the school's network; no independent (for example through a 3G/4G connection) access is permitted.
9. The accessing, or updating, of social media platforms is not permitted unless it is part of a structured educational activity.
10. The exception to the above is that pupils in the Sixth Form are allowed to use their devices only in their Common Room. If they use their devices outside of the Sixth Form Common Room, they should expect the same sanction as the rest of the school.
11. Pupils should be aware that under no circumstances should they enter an examination venue with a device, even if it is switched off. To do so will lead to disqualification from that examination and potentially other examinations.
12. Pupils should note that the use of all devices on school premises is subject to the school's Technology Acceptable Usage policy.

BYOD Guidelines for Staff

1. Staff personal BYOD should be switched off (or in silent mode) during lessons, or at times where they are responsible for the supervision of students.
2. Staff should not use a personal mobile digital device, or similar, during lessons (or when supervising students) to receive or send personal calls, texts or post content to personal social media platforms.
3. If a member of staff feels that it is necessary to be available to receive a personal call or text on a personal mobile device during a lesson, for which there may be exceptional circumstances, they should explain this to their line manager beforehand.
4. Staff should not use a personal mobile digital device, or similar, during lessons (or when supervising students) to access online resources, emails, apps or similar, unless it is considered that the outcome is essential to pupil learning and cannot be sourced through the school network (in which case, pupils should be made aware that the mobile device has been used for this educational purpose).

5. Staff must, where possible, only use school devices to take images of students. If this is not feasible then personal devices can be used but images must be deleted as soon as possible after uploading to school systems.
6. Staff should endeavour to make any personal calls on their own mobile telephone, or similar, in a discreet fashion and away from any pupil area, for example in the Staff Room or in an office, behind closed doors.
7. Staff should not give out their personal mobile phone numbers, or other communication contact information, to students.
8. Inappropriate use of BYOD is a serious offence; cases of misuse could lead to disciplinary action being taken against the individual concerned.

Additional guidelines for staff use (photographs and videos)

Dunottar School recognises that it is not always practical for teachers to borrow the school camera for events and trips and that photographs of such activities form an integral part of key publications such as the Newsletter. Staff are allowed to use their own devices to take photographs of children, if it is not practical to borrow the school camera or use their school iPad (**having received authorisation** from their line manager and fully understanding the implications of devices which are synchronised to online storage).

Staff must under no circumstances ever use any photographs of students for anything other than strictly professional purposes. They must never upload photographs or videos of any students onto the internet or social media site unless in line with the Social Media Policy. Use of photographs of students, where parents have given consent, can be uploaded onto the school's own website or other school managed social media platforms.

If staff are using social media websites such as Facebook or Twitter e.g. to set up subject pages, they should not upload any photographs of students themselves, unless they are following strict school guidelines and are aware of which students should not be photographed. Further details can be found in the school's Social Media Policy.

After taking photographs of students with their own devices, staff should not store these for any longer than necessary, and once copied onto the school network should be deleted from all personal devices, including online storage.

Before printing any photographs of students in any external publication (e.g. local or national newspapers), parents must give permission for the student's photograph and/or name to be used.

Filtering Policy

Filtering Policy Statement

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 e-safety and acceptable use. It is important that Dunottar school has a filtering, monitoring and reporting policy to manage the associated risks and to provide preventative measures which are relevant to the situation and context in Dunottar school.

This policy applies to all members of our school community, including those in our Sixth Form.

Dunottar School seeks to implement this policy through adherence to the procedures set out in the rest of this document. The school is fully 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.

This document is available to all interested parties on the school's website and on request from the School Office. It should be read in conjunction with:

- E-Safety Policy
- Pupil Acceptable Use Agreement
- Staff Acceptable Use Agreement
- Information Technology Policy
- Digital BYOD Policy
- Electronic Devices- Searches and Deletion Policy

This document is reviewed annually by the Deputy Head Pastoral and the Network Manager, or as events or legislation changes require. The next scheduled date for review is October 2023.

Introduction

The monitoring of the Internet is a critical element of any filtering policy as it highlights weaknesses in the filtering device, unusual activity by users, interest in extremist material or self-harm. This monitoring is normally surfaced through regular reports to specific staff members who understand student context and the curriculum. These reports should be regularly reviewed (weekly) and appropriate actions documented. Expect significant false positives when initially implemented.

Dunottar School uses the Fortinet FortiGuard Web Filtering Service. It comprises of a hardware device and an associated software Application with it.

Users are aware of the flexibility provided by Dunottar 's Filtering services. Staff members use this flexibility to meet their teaching needs and maximise the use of the new technologies.

Dunottar School decided:

- They will use the provided filtering service to allow flexibility for sites to be added or removed from the filtering list for their organisation.
- To introduce differentiated filtering for different groups / ages of users.
- To remove filtering controls for some internet use (e.g. social networking sites) at certain times of the day or for certain users.
- The head teacher has the control to accept or reject a requests from staff with regards to removing filtering controls for some sites.
- Securus system is a user monitoring system used to supplement the filtering system. It captures screens of users working windows that has any inappropriate text or images. It saves it to a cloud based storage location. A console control is used to monitor the activities of users by viewing the screen captures. Administrators can decide whether it is a genuine breach of behaviour or a false positive captures.

Day to day requests are viewed and assessed by the Network Manager. When necessary a consultation with the Deputy Head Pastoral is made before taking the final decision. If a decision is not reached the Headmaster, will then get consulted to give the final decision.

Key Personnel

Mr Thomas Stevens (Network Manager)

Mr John Weiner (Deputy Head)

Mr Dan Hawker (LGB)

Key personnel providing e-safety training

Mr James Garnett (IT Director, United Learning)

Responsibilities

The responsibility for the implementation of the school's filtering policy will be held by (Network Manager). 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 there is a system of checks and balances and to protect those responsible, changes to the school filtering service are:

- **Logged in change control logs (viewable on the system)**
- **Reported and authorised by a second responsible person prior to change (Deputy Head) depending on the severity of the request.**

All users have a responsibility to report immediately to the Designated Safeguarding lead 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.

Filtering in Practice

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 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.

- Any breach of the filtering policy will result in action in live with the United Learning Disciplinary Policy
- The school has provided enhanced / differentiated user-level filtering through the use of the Fortiguard 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 Head teacher (or other senior leader).
- BYOD 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 at the discretion of the Network Manager and if necessary in consultation with the E-Safety Co-ordinator, John Weiner.

The E-Safety Co-ordinator's role is to ensure support for the Network Manager or any other member of staff, should any exposure to distressing or inappropriate unfiltered materials occur.

Education / Training / Awareness

Pupils / students will be made aware of the importance of filtering systems through the e-safety education programme (through PSHE and Computing lessons). They will also be warned of the consequences of attempting to subvert the filtering system.

Parents / Carers will be informed of the school's filtering policy through the Pupil Acceptable Use Agreement and through e-safety awareness sessions and communications from the school.

Staff users will be made aware of the filtering systems through

- the Staff Acceptable Use Agreement
- induction Training
- staff meetings, briefings and staff training sessions.

Changes to the Filtering System: Procedures

- When users come across a blocked site the system advises the category that is preventing them access to it. If they believe they should have access to it they should send an email to the Network Manager asking for the site to be unblocked or log a IT helpdesk ticket.
- When a request is made, the Network Manager checks the site and advise the users that the site is unblocked. If there is uncertainty as to the suitability of the site requested to be unblocked, then permission must be sought from the Deputy Head Pastoral to ensure it complies with the eSafety policy.
- Communications usually happens by emails. Any site that is unblocked, a description of the request with the date and name of staff members/students/department is put on the 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 (Thomas Stevens) who will decide whether to make school level changes (as above).

Monitoring

Securus is Dunottar's monitoring system that monitors all activities of all users and takes a snapshot of their screens. The Network Manager keeps a good check on the screen captures on a daily bases and reports are sent through to the E-Safety Coordinator on a weekly basis. In the event that material is discovered which contravenes the E-Safety and Safeguarding (Child protection) policies, the Network Manager will report immediately to the E-Safety Co-ordinator.

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 E-Safety Policy and the Pupil and Staff Acceptable Use Agreement.

Audit / Reporting

Logs of filtering change controls and of filtering incidents will be made available to the E-Safety Coordinator Deputy Head, John Weiner as and when they occur.

E-Safety Group

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 Dunottar School may question whether the 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).

E-Safety Policy

E-Safety Policy Statement

The e-safety policy is a key element of the IT Policy as it is about the safe and responsible and ethical use of online technologies. It covers accessing online resources through computers, tablets, smart phones and any other internet enabled device safely and effectively. In conjunction with the social media Policy, it includes new social media tools and other emerging trends. It should cover a range of issues and not condemn the use of tools but rather address how to use them safely. This should include how to comment appropriately in many different forums, including social media and not being just a bystander. An essential part of this is how to report concerns, online and offline.

This policy applies to all members of Dunottar School who have access to and are users of school ICT systems, both in and out of the school.

Dunottar School is fully committed to ensuring the application of the E-Safety Policy and other related technology policies are non-discriminatory in line with the UK Equality Act (2010). Further details are available in the school's Equal Opportunity Policy document.

Dunottar School seeks to implement this Policy through adherence to the procedures set out in the rest of this document.

In line with our Provision of Information Policy, this document is available to all interested parties on our website and hard copies are available, on request, from the school main office.

This e-safety policy should be read in conjunction with other policies with the over-arching Technologies Policy but with particular reference to the IT Policy, BYOD Policy, Social Media Policy and Internet Filtering Policy.

The next date for review is October 2022 or when events or legislation require.

Key Personnel

- Mr Thomas Stevens (Network Manager)
- Mr John Weiner - E-Safety Co-ordinator (Deputy Head Pastoral)
- Mr Dan Hakwer (LGB Member)

Key personnel providing external e-safety training

- Mr James Garnett (IT Director, United Learning)

Area of risk:

Communicating with children electronically

Using online services and sites, not provided by Dunottar School, to communicate between a teacher and a student may put one or both participants at risk. This is because; it is not open and transparent, there is no audit trail, Dunottar School do not control the communication channel so cannot access the data, it is impossible to monitor.

E-Safety in the Curriculum

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum. E-safety should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned e-safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited
- Key e-safety messages will be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- Students will be taught in all lessons to be critically aware of the materials/ content they access on-line and be guided to validate the accuracy of information when using technology.
- Students will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students understand and sign the Student Acceptable Use Agreement and are encouraged to adopt safe and responsible use both within and outside school
- Staff will act as good role models in their use of digital technologies, the internet and BYOD.
- In lessons where internet use is pre-planned, it is best practice that students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Staff should be mindful that they must differentiate between different Year groups when planning lessons using the internet.
- Where students are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the students visit. Additional monitoring of individual internet use is also in place via Securus.

E- Safety and Staff

All staff must read and sign the ICT Acceptable Use Policy for Staff, before using any school ICT resource. The school will maintain a current record of all staff who are granted access to school ICT systems. Any person not directly employed by the school will be asked to sign the ICT Acceptable Use Policy for Staff before being allowed to access the internet from the school site.

All staff will be directed to the School's E-Safety Policy, and related policies and procedures, and their importance explained. Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential. Staff that manage filtering systems or monitor ICT use will be supervised by the senior management and have clear procedures for reporting issues.

E- Safety and Students

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in e-safety is therefore an essential part of the school's e-safety provision. Dunottar School provides children and young people help and support so they can recognise and avoid e-safety risks, build their resilience and use technology responsibly.

All students must read and sign the ICT Acceptable Use Policy for Students, before using any school ICT resource. The school will maintain a current record of all students who are granted access to school ICT systems.

The School controls access to social networking sites and considers how to educate students in their safe use, such as the use of passwords. This control may not mean simply blocking every site, which is usually counter-productive; it is often more effective and valuable to monitor and educate students in their use. Newsgroups will be blocked unless a specific use is approved.

Students are advised never to give out personal details of any kind which may identify them or their location. Students must not place personal photos on any social network space provided in any school learning platform or application. In addition, students and parents are advised that the use of social network spaces outside school brings a range of opportunities; however, it does present dangers for primary and secondary aged students.

Students are advised to use nicknames and avatars when using social networking sites and to consult adults at once if someone they have encountered online requests to meet them.

E- Safety and Parents / carers

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- Letters
- Parental evenings
- High profile events, campaigns and visiting speakers e.g. Dunottar's 'Virtually safe' Safer Internet Week
- Reference to the relevant web sites / publications e.g. CEOP (www.ceop.police.uk) and Child line (www.childline.org.uk) which can also be found via the school website

E-safety Information

Internal resources

e-safety information can be accessed by students and teachers via the school website and on the United Hub.

External resources

External sources of reliable information on the safe use of the internet, training resources, parental information sites, can be accessed on the useful links page of the school website.

Reporting Procedures

Staff are encouraged to use the helpdesk system to alert members of the IT department. Students should report any instances of occasions where unsuitable or inappropriate material is accidentally viewed directly to their teacher who will then pass it on to the e-safety co-ordinator.

Monitoring Success

In order to monitor the success of e-safety in the school Dunottar school:

- Gets weekly search query reports which show what is being looked at on the internet

Electronic Devices Policy- Searches and Deletion

Electronic Devices Policy Statement – Searches and Deletion

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 Deputy Head Pastoral John Weiner who will report to the Local Governing Body on its implementation on a regular (annual) basis. The date of the next review is Aug 2023.

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
  The IT policies

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 Head teacher (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 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 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:

John Weiner Deputy Head (Pastoral) and Janine Hislop Deputy Head (Academic)

The Head teacher 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.

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 Head teacher 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.

If there is any suggestion that the material to be searched may include sexual or graphically disturbing images staff must not view that material.

Search:

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

Pupils 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 BYOD Guidance for Pupils Section of the IT policy.

If Pupils 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- **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. 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 the 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, John Weiner DSL (Deputy Head pastoral) and Janine Hislop 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 John Weiner DSL (Deputy Head Pastoral) or Janine Hislop 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 John Weiner and Thomas Stevens 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 John Weiner / E-Safety Committee / E-Safety Governor Gary Richards at regular intervals.

Name of owner/author	John Weiner, Deputy Head Pastoral (owner from September 2023) in consultation with the School Network Manager Marc Broughton 2019	Mark Tottman 2019 R.Cole Sept 2016
This document was created in Sept 2019 by merging our existing updated Technology Policies		
LGB Member with Responsibility Dan Hawker (October 2022)		
Date Document Reviewed	November 2020	S.Thorne / M.Broughton
Date Document Reviewed	October 2022	M.Broughton, Deputy Head Pastoral in consultation with the School Network Manager
Date Document Reviewed	September 2023	J.Weiner, Deputy Head Pastoral in consultation with the School Network Manager
Next Review Date	September 2024	Or when event or legislation require