Lancaster Royal Grammar School

POLICY STATEMENT

Number	Date Approved by Governing Body
50	July 2018

Digital and Social Media Policy

Background/Rationale

New technologies have become integral to the lives of many people of all ages in today's society, both within schools and in their lives outside school.

The requirement to ensure that all members of the school community are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound.

Many of these risks reflect situations in the off-line world and it is essential that this policy be used in conjunction with other school policies (e.g. behaviour, anti-bullying, and child protection policies).

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential that good educational provision is made to build pupils' resilience to the dangers to which they may be exposed, so that they have the confidence and skills to deal with these risks.

All staff, students, and parents/carers should be aware of the potential for serious child protection issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

Scope of the Policy

This policy applies to all members of the school community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of the school. This policy also applies to the use of personal technologies in school.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour of Pupils Policy.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the roles and responsibilities of individuals within the school. While these roles are discrete it is acknowledged that individuals will work closely together to promote a coherent whole school approach to e-safety.

The Governors are responsible for:

- the approval of the Digital and Social Media Policy and for reviewing the effectiveness of the policy, this will be carried out by the Governors' Personnel Committee
- appointing an E-Safety Governor

The E-Safety Governor will:

- liaise with the E-Safety Co-ordinator and Deputy Head (Pastoral & Boarding)
- report to the Governors' Personnel Committee as necessary

The Headmaster:

- is responsible for ensuring that the school policies reflect the requirements contained within the relevant legislation.
- has a duty of care for ensuring the safety of members of the school community
- is responsible for ensuring that the E-Safety Coordinator and other relevant staff receive suitable CPD to enable them to carry out their roles
- is responsible for the procedures to be followed in the event of a serious allegation being made against a member of staff

Deputy Head (Pastoral & Boarding) & Pastoral Leaders (including Form Tutors):

- are responsible for the investigation of reported e-safety incidents

E-Safety Coordinator:

- is responsible for the co-ordination of e-safety education, and pupil and parent awareness
- is responsible for leading the review of the school e-safety curriculum
- will receiving e-safety incident reports to inform future e-safety developments
- will liaise with the E-Safety Governor and Deputy Head (Pastoral & Boarding) to discuss current issues and review incident logs
- will attend relevant meeting of Governors
- will report to the Senior Leadership Team
- will receive regular updates regarding eSafety trends and new issues from official sources e.g. the Child Exploitation and Online Protection service (CEOP)
- is responsible for ensuring staff receive relevant awareness training, and have an up to date awareness the current school policy and practices

Assistant Head (ICT & Systems) is responsible for ensuring:

- that the school community are aware of the safe and appropriate use of school equipment and systems,
- that staff have read, understood and signed the school Staff Acceptable Use Policy (AUP)
- that parents acknowledge receipt of and support the Student Acceptable Use Policy (AUP)
- that the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- that users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed
- that the use of the network / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported for investigation
- that teaching and support staff report any suspected misuse or problem using the school's behavioural incident reporting system
- that digital communications with students is on a professional level and it is advised to be only carried out using official school systems detailed in this policy
- that ICT activity in lessons, extracurricular and extended school activities is monitored
- that the school infrastructure / network is as safe and secure as is reasonably possible
- the school's ICT systems are be managed in ways that ensure that the school meets the e-safety technical requirements outlined in any relevant Local Authority E-Safety Policy and guidance
- that there are regular reviews and audits of the safety and security of school ICT systems
- that servers, wireless systems and cabling must be securely located and physical access restricted
- all users will have clearly defined access rights to school ICT systems, and details of the access rights available to groups of users are recorded

Staff *and Volunteers*:

- are responsible for using the school ICT systems and their own devices in accordance with the Staff Acceptable Use Policy and the Digital and Social Media Policy
- are responsible for ensuring that their digital communications with members of the school community are on a professional level and should only be carried out using official school systems

Students:

- are responsible for using the school ICT systems and their own devices in accordance with the Student Acceptable Use Policy and the Digital and Social Media Policy
- are responsible for ensuring that their digital communications with members of the school community are on a professional level and should only be carried out using official school systems

Parents/Carers:

- should play an essential role in the education of their children and in the monitoring / regulation of their child's on-line experiences
- should ensure that their children understand the need to use the internet / mobile devices in an appropriate way
- should endorse the Student Acceptable Use Policy
- access the online school systems in accordance with the relevant school Acceptable Use Policy

Education & Training

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. E-Safety education will be provided through a planned e-safety programme delivered through the Values programme, e-safety workshops, assemblies and tutorial activities, Safer Internet Week, Anti-Bullying Week and in all lessons as appropriate. The Acceptable Use Policy will be published on the school's website and on the VLE.

The aims of digital safety programmes are detailed in the relevant planning documentation.

Parents / Carers

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

- letters, newsletters, and the school's web site
- Parents' Digital Safety Awareness Evenings
- providing a copy of the Acceptable Use Policy

Staff

It is essential that all staff receive Digital Safety training in conjunction with child protection training. All new staff should ensure that they fully understand the school Digital and Social Media Policy and Acceptable Use Policies.

Governors

The E-Safety Governor should take part in e-safety training / awareness sessions, and participate in school training / information sessions for staff and parents.

Bring Your Own Device

In terms of this policy devices are defined as an electronic technology which may have internet connectivity, including phones, tablets, computers, smart watches, gaming devices and other similar devices.

The educational opportunities offered by mobile technologies are being expanded as a wide range of devices, software and online services become available for teaching and learning, within and beyond the classroom. The school permits users to bringing their own technologies to school in order to provide a greater freedom of choice and usability. However, the school has a differentiated approach to the use of these devices during the school day as follows:

Year 7: Are not permitted to use their devices during the school day, nor on the school site, their devices must be switched off and in their bags at these points. A teacher may give permission for these students to use their devices in lessons for a purpose which supports their learning.

Year 8 (Michaelmas and Lent Terms): Are not permitted to use their devices during the school day, nor on the school site, their devices must be switched off and in their bags at these points. A teacher may give permission for these students to use their devices in lessons for a purpose which supports their learning.

Year 8 (Summer Term): At the discretion of the Head of Year 8 & 9 and at the completion of the 'Earn Your Licence' Values module, Year 8 students will be allowed to use their devices under the same rules as Years 9 to 13 (detailed below). This is a probationary period and subject to review.

Years 9 to 13: Students are only permitted to use their mobile devices during break and lunchtime, and with the permission of their teacher in lessons in order to support their learning. The following rules apply at all points in the school day:

- The use of a mobile device is prohibited when travelling around the site and crossing roads.
- The use of a mobile devices is prohibited in toilets and changing rooms.
- At no point must any member of the school community use their device in a way which disrupts teaching and learning, brings the school into disrepute, or adversely affects the safety and wellbeing of members of the school community.
- The use of mobile devices must not contravene the school's behaviour, bullying or Acceptable Use Policy
- Personal mobile devices must not be used for the taking of photographs or video of members of the school community. Nor will these features be used by students for other purposes on the school site without the permission of a member of staff.

Consequences for Students

The devices of students who fail to maintain these principles will be confiscated by a member of staff. The school operate a next day return on confiscated devices; confiscated devices may be collected the following morning from City View. Exceptions will be made for students with Health Care Plans who can pick up their phone at the end of the school day. Students who've had their device confiscated and need to contact their parents or carers may do this from any of the school receptions. In exceptional circumstances a school phone may be loaned to a student in order to safeguard them on their journey home. This phone must only be used by the student for the purpose of keeping them safe on their journey home, it must be returned to school the next day. Students who have had their phone confiscated on Friday may choose to collect their phone from the member of staff leading Friday Detention at 4.45pm from City View, or to collect it the following Monday.

Before a confiscated phone is returned the student will have to demonstrate their understanding of the rules. In some instances, parents may be asked to collect the device and the student may forfeit the right to use their phone in school.

Mobile devices are allowed in school on the understanding that they are the responsibility of the individual. The school can take no liability for their loss or damage. If a member of staff confiscates a device they must take measures to protect the student's device and ensure its safe return at an appropriate point.

All users must adhere to this policy regardless of who owns the device being used, and the following principles apply:

- The school has a set of clear expectations and responsibilities for all users, detailed in this policy
- The school adheres to the Data Protection Act principles
- All users are provided with and must act within the Acceptable Use Agreement
- Where possible these devices will be covered by the school's normal filtering and monitoring systems, while connected to the school's network

Searching Mobile Devices & Deletion of Data

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.

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 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. These items are detailed in the Behaviour of Pupils policy and this policy.

The act allows authorised persons staff 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 Headteacher has authorised the following members of staff to carry out searches for and of electronic devices and the deletion of data / files on those devices: members of the Senior Leadership Team, Heads of Years, and Housemasters.

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

Searching Mobile Devices & Deletion of Data (conducting searches)

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

Authorised staff (defined 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) 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 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 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.**

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.

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

Searching Mobile Devices & Deletion of Data (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.

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.

Digital Images

The development of digital imaging technologies has created significant benefits to teaching & learning and school marketing, allowing staff and student's instant use of images that they have recorded themselves or downloaded from the internet. However, in order to safeguard members of the school community the following guidelines must be followed:

- Digital images (including video) of members of the school community should only be taken on school equipment; the personal equipment of members of the school community should not be used for such purposes. To this end, the school will endeavour to make equipment available for staff to use
- When school equipment is being used to record digital images, a responsible person will ensure that any images are secured in line with this policy. The responsible person is identified as the member of staff having ownership of the device (e.g. the Head of Department), or the individual authorised to use school equipment at that time
- The photographing or filming of members of the school community without their permission is prohibited (parents will choose whether or not to consent to their son's or daughter's image being used for educational and marketing purposes)
- The identities of members of the school community must be safeguarded at all times, to this end students' full names will not be used in any public space, particularly in association with photographs
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images.
- Care should be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute. Images must not be taken of sensitive events e.g. images of trauma or injury
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published or made publicly available on social networking sites, nor should parents / carers comment on any activities involving other students in the digital / video images

Communicating with Students

When using communication technologies the school considers the following as good practice:

- All members of the school community a must follow the Acceptable Use Policy when communicating using school systems
- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and students should therefore use the school email service as the main method of communicating with others when in school, or on school systems (e.g. by remote access). Communication involving the personal email accounts of staff or students is prohibited
- In some circumstances, such as educational visits or sporting fixtures, communication using official school mobile phones is permitted. Nevertheless the tone of this communication is still bound to the Acceptable Use Policy
- The use of social media to broadcast information to students must abide by this policy, the law, and the corporate restrictions on users. Students must never be expected to give a false account of themselves in order to access the systems we may use

The Use of Social Media

With an increase in use of all types of social media for professional and personal purposes it is essential that members of the school community manage risk and behaviour online. Expectations for teachers' professional conduct are set out in 'Teachers Standards 2012'.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:

- Training available relating to: acceptable use; social media risks; checking of settings; data protection; reporting issues
- Clear reporting guidance, including responsibilities, procedures and sanctions

Staff should ensure that:

- No reference should be made in personal social media accounts to students, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information
- They maintain a clear distinction and separation between their professional and personal online personas, and that connections are not made between the personal online personas of staff and students.

Social Media for Professional and Educational Purposes

The school endeavours to make the most of social media for professional and educational purposes, while meeting its safeguarding obligations. The school's use of social media for professional purposes will be reviewed regularly to this end. Where social media is being used, the following should apply:

- Social media accounts set up for discrete aspects of the school community e.g. academic departments or sports teams, should be logged with the Network Manager, along with a record of who the responsible person for the account is
- The responsible person is responsible for the activity and use of the account
- The responsible person must make sure the account conforms to school policies
- The responsible person must make sure the necessary steps are taken to secure the account, and that only authorised staff can use the account
- The responsible person must liaise with the Marketing Officers to maintain the schools corporate aesthetic

Users of social media accounts which are officially linked to the school must not bring the school into disrepute by associating, directly or indirectly, with users whose online activity and use may be deemed to do so.

Members of the school community must not create unofficial accounts linked to the school, impersonate members of the school community, or aim to deceive members of the school community or the public.