E-SAFETY POLICY

This policy applies across the School from Year 1 and upwards.

INTRODUCTION

It is the duty of Newcastle School for Boys to ensure that each pupil in its care is safe; and the same principles apply to the digital world as apply to the real world.

IT and online communications provide unrivalled opportunities for enhanced learning in addition to traditional methods, but also pose greater and subtler risks to young people. Our pupils are therefore taught how to stay safe in the online environment and how to mitigate risks including, but not limited to, the risk of identity theft, bullying, harassment, grooming, stalking and abuse.

New technologies are continually enhancing communication, the sharing of information, learning, social interaction and leisure activities. Current and emerging technologies used in and outside of school include:

- Websites;
- E-mail and instant messaging;
- Blogs;
- Social networking sites;
- Chat rooms;
- Music/video downloads;
- Gaming sites;
- Text and picture messaging;
- Video calls;
- Podcasting;
- Online communities via games consoles; and
- Mobile internet devices such as smart phones and tablets.

This policy, supported by the ***Policy on pupils use of ICT mobile phones and other electronic devices***, is implemented to protect the interests and safety of the whole school community. It aims to provide clear guidance on how to minimise risks and how to deal with any infringements. It is linked to the following school policies:

- ***Safeguarding and child protection policy***
- ***Health and safety (main) policy***
- ***Behaviour management policy***
- ***Anti-bullying policy***
- ***Senior and Junior School rules for responsible use of the School's computer network***

- ***Staff code of conduct for use of the school computer network***
- ***iPad user agreement and acceptable use policy***
- ***Data protection-pupil***
- ***Data protection - staff***
- ***BYOD wireless network policy and***
- ***Personal, social and health education policy***

Whilst exciting and beneficial both in and out of the context of education, much IT, particularly online resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these internet technologies.

At Newcastle School for Boys, we understand the responsibility to educate our pupils on e-safety issues; teaching them the appropriate behaviours and critical thinking skills necessary to enable them to remain both safe and within the law when using the internet and related technologies in and beyond the classroom.

This policy, the ***iPad User Agreement and Acceptable Use Policy*** and the ***BYOD Wireless Network Policy*** cover both fixed and mobile internet devices provided by the school (such as PCs, laptops, webcams, tablets, whiteboards, digital video equipment, etc.), as well as all devices owned by pupils and staff brought onto school premises (personal laptops, tablets, smart phones, etc.).

ROLES AND RESPONSIBILITIES

The Designated Safeguarding Lead (DSL) and IT manager have responsibility for ensuring this policy is upheld by all members of the school community. They will keep up-to-date on current e-safety issues and guidance issued by organisations such as the local authority, CEOP (Child Exploitation and Online Protection), Childnet International and the Newcastle Safeguarding Children Board.

As with all issues of safety at this school, staff are encouraged to create a talking culture in order to address any e-safety issues which may arise in classrooms on a daily basis.

Newcastle School for Boys believes that it is essential for parents/carers to be fully involved with promoting e-safety both in and outside of school. We regularly consult and discuss e-safety with parents/carers and seek to promote a wide understanding of the benefits and risks related to internet usage.

STAFF AWARENESS

All teaching staff receive regular information and training on e-safety issues in the form of INSET training and are made aware of their individual responsibilities relating to the safeguarding of children within the context of e-safety.

All staff working with children are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following school e-safety procedures. These behaviours are summarised in the ***Staff code of conduct for use of the school computer network and the internet*** which must be signed and returned before use of technologies in school.

Teaching staff are encouraged to incorporate e-safety activities and awareness within their subject areas and through a culture of talking about issues as they arise. They should know what to do in the event of misuse of technology by any member of the school community.

A record of concern must be completed by staff as soon as possible if any incident relating to e-safety occurs and be provided directly to the school's Designated Safeguarding Lead (DSL).

E-SAFETY IN THE CURRICULUM AND SCHOOL COMMUNITY

IT and online resources are used increasingly across the curriculum. We believe it is essential for e-safety guidance to be given to pupils on a regular and meaningful basis. We continually look for new opportunities to promote e-safety and regularly monitor and assess our pupils' understanding of it.

Every fifteen days, boys have to sign an electronic agreement in order to be allowed access to the network to remind them to follow the School's IT guidelines.

The School provides opportunities to teach about e-safety within a range of curriculum areas and IT lessons. Educating pupils on the dangers of technologies that may be encountered outside school will also be carried out via PSHE, as well as informally when opportunities arise.

At age-appropriate levels, starting from Year 1, boys are given advice on how to look after their own online safety. As the boys grow older they are taught about recognising online sexual exploitation, stalking and grooming, the risks, and of their duty to report any such instances they or their peers come across. Pupils can report concerns to the DSL and any member of staff at the school.

Boys are also taught about relevant laws applicable to using the internet; such as data protection and intellectual property. Boys are taught about respecting other people's information and images, etc. through discussion and classroom activities.
Boys should be aware of the impact of cyber-bullying and know how to seek help if they are affected by these issues (see also the school's ***Anti-bullying policy***). Boys should approach the DSL as well as parents, peers and other school staff for advice or help if they experience problems when using the internet and related technologies.

USE OF SCHOOL AND PERSONAL DEVICES

Staff

School devices assigned to a member of staff as part of their role must have a password or device lock so that unauthorised people cannot access the content. When they are not using a device staff should ensure that it is locked to prevent unauthorised access.

All personal devices need to be enrolled with the School's ICT manager before access to the school's Wi-Fi can be granted. This process ensures that staff's personal devices are subject to the school's filtering restrictions.

Staff should not give their personal mobile phone numbers or e-mail addresses to pupils, nor should they communicate with them by text message or personal e-mail. If they need to speak to a pupil by telephone, they should use one of the School's phones and e-mail using the school system.

Pupils

Newcastle School for Boys ('the School') provides a bring your own device (BYOD) wireless network which is made available to staff and students who have a compatible wireless device to enhance their professional and educational activities including learning, teaching, research, administration and management.

Use of this provision is governed by the School's ***iPad User Agreement and acceptable use policy*** and by logging onto the network the user is deemed to have agreed to abide by.

USE OF INTERNET AND E-MAIL

Staff

Staff must not access social networking sites, personal e-mail, any website or personal email which is unconnected with school work or business whilst teaching or in front of pupils.

When accessed from personal devices/off school premises, staff must use social networking sites with extreme caution, being aware of the nature of what is published online and its potential impact on their professional position.

There is strong anti-virus and firewall protection on our network and, as such, it may be regarded as safe and secure. Staff should be aware that e-mail communications can be accessed.

Staff must immediately report to IT Manager the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.

Any online communications must not either knowingly or recklessly:

- place a child or young person at risk of harm;
- bring Newcastle School for Boys into disrepute;
- breach confidentiality;
- breach copyright;
- breach data protection legislation; or do anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example by:

- making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age;
- using social media to bully another individual; or
- posting links or material which is discriminatory or offensive.

Under no circumstances should school pupils or parents be added as social network 'friends'.

Any digital communication between staff and pupils or parents/carers must be professional in tone and content. Staff should not contact a pupil or parent/carer using a personal email address. The school ensures that staff have access to their work email address when offsite, for use as necessary on school business.

Pupils

All boys in the Senior School are issued with their own personal school e-mail addresses for use on our network and by remote access. Access is via a personal login, which is password protected. This official email service may be regarded as safe and secure, and must be used for all school work, assignments/research/projects. Pupils should be aware that email communications can be accessed.

There is strong anti-virus and firewall protection on our network. Spam emails and certain attachments will be blocked automatically by the email system. If this causes problems for school work/research purposes, pupils should contact the IT Manager for assistance.

Pupils should immediately report, to the IT Manager/or another member of staff the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.

Pupils must report any accidental access to materials of a violent or sexual nature directly to the IT Manager or another member of staff. Deliberate access to any inappropriate materials by a pupil will lead to the incident being recorded on their file and will be dealt with under the School's ***Behaviour management policy***. Pupils should be aware that all internet usage via the School's systems and its Wi-Fi network is monitored.

Certain websites are automatically blocked by the School's filtering system. If this causes problems for school work/research purposes, pupils should contact the IT Manager for assistance. The IT Manager in consultation with the Designated Safeguarding Lead will make a decision on the appropriateness of such sites.

DATA STORAGE

The school takes its compliance with the Data Protection Act 1998 seriously. Please refer to ***Data protection policy - staff*** for further details.

Staff may only take information offsite when authorised to do so, and only when it is necessary and required in order to fulfil their role. No personal data of staff or pupils should be stored on personal memory sticks.

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of IT must be immediately reported to the IT manager.

PASSWORD SECURITY

Pupils and staff have individual school network logins, email addresses and storage folders on the server. Staff and pupils are regularly reminded of the need for password security.

All pupils and members of staff should:

- use a strong password (usually containing eight characters or more, and containing upper and lower case letters as well as numbers), which should be changed at least annually;
- not write passwords down; and
- should not share passwords with other pupils or staff.

SAFE USE OF DIGITAL AND VIDEO IMAGES

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying, stalking or grooming to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing their own images on the internet (e.g. on social networking sites).

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 is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published on blogs or social networking sites, etc., nor should parents/carers comment on any activities involving other pupils in the digital/video images.

Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow this policy and the School's ***Staff code of conduct for use of the school computer network*** and ***Policy on taking, storing and using images of children*** concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment: personal equipment should not be used for such purposes. Care should be taken when taking digital/video images that

pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

Pupils must not take, use, share, publish or distribute images of others without their permission.

Written permission from parents or carers will be obtained before photographs of students/pupils are published on the school website.

Photographs published on the school website, or displayed elsewhere, that include pupils, will be selected carefully and will comply with good practice guidance on the use of such images. Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

COMPLAINTS

As with all issues of safety at Newcastle School for Boys, if a member of staff, a pupil or a parent/carer has a complaint or concern relating to e-safety prompt action will be taken to deal with it. Complaints of this nature should be addressed to the DSL in the first instance, who will undertake an immediate investigation and liaise with the leadership team and any members of staff or pupils involved. Please see the ***Complaints procedure*** for further information.

Incidents of or concerns around e-safety will be recorded and reported to the school's the Designated Safeguarding Lead, in accordance with the School's ***Safeguarding and child protection policy***.

Reviewed: September 2017
Revised and updated: September 2017
DT