Author: CHD
Date: September 2021
Review Date: September 2022

GOSFORTH GROUP
E-SAFETY POLICY

1 PURPOSE

1.1 This policy guidance aims to help everyone within Gosforth Group schools understand their roles and responsibilities in ensuring the safe and acceptable handling/use of information technologies.

2 ROLES AND RESPONSIBILITIES

2.1 Applicable to all users of technology and connected systems:

2.1.1 Deliberate unlawful/inappropriate material must not be viewed/stored/distributed on the school system. This includes material which is in violation of any law/regulation or which can be considered by any reasonable person in its context to:

- be defamatory;
- be violent;
- be offensive;
- be abusive;
- be indecent or obscene;
- be discriminatory;
- incite hatred;
- constitute bullying and/or harassment; and
- breach anyone's confidence, privacy, trade secrets or copyright.

2.1.2 If someone has stated that they do not wish to receive emails from you then you must refrain from sending further e-mails to them. You must not use the school's email systems for 'spamming' purposes (the use of email to send unwanted/junk/advertising content to multiple recipients).

2.1.3 Particular care should be taken whenever you choose to use your own personal technologies in our work environment and ensure that other people, including children, are not able to see personal contents which you would deem private or sensitive… keeping professional and private lives separate.

2.1.4 You must ensure that your work computer account is not misused so you should not share your username or password with anyone. All Internet and network use of systems are subject to monitoring by the school and this may be traced back to you. Everyone is responsible for ensuring information systems are secure, safe and used to benefit all. You should be aware that disciplinary/civil/criminal action might arise if any user is found to be deliberately accessing material described above. Similarly, unauthorised or deliberate illegal access to or use of data, systems or networks is prohibited and may also result in disciplinary/civil/criminal action.

2.2 APPLICABLE TO THE ORGANISATION AS A WHOLE:

2.2.1 The Principal is ultimately responsible for network activity and e-safety in the school.

E-safety is led by an identified person who has designated responsibility for it. The school supports training for this role. In Gosforth Group schools the designated staff are the Safeguarding and Deputy Safeguarding Leads who can be contacted for further advice and support.

2.2.2 We connect to broadband via Filtered Internet Services to reduce the risk of anyone accessing illegal/unsuitable sites. This covers all users connected to our networks. Any user who accidentally accesses material they deem to be inappropriate on their own machine (or notices the same on others' machines) must report this to their e-safety lead officer to help protect themselves, other people and the school.

2.2.3 We encourage and develop:

- ongoing e-safety training to the wider community;
- the safe use of social networking sites; and
- secure 'guest' access to our networks of an individual's own learning device, be that a laptop, smartphone or portable games console.

2.2.4 **The Principal is** responsible for having practices/procedures/staffing in place to ensure that:

- all computers (and other ICT equipment) have fully up to date anti virus and anti spam protection;
- all software is properly licensed for use within school;
- appropriate measures are in place to prevent the bypassing of filtering or network security systems;
- devices not owned by the organisation (such as personally-owned devices) cannot connect directly to secure systems (but may connect through "guest" access systems, where available);
- all users have personal, identifiable and secure logons to network resources so that illegal/inappropriate use can be identified to a particular user. Shared passwords/logons should not be used;
- all users of our systems have regular updates where the latest information surrounding being e-safe can be shared; and
- all users are aware of how to report suspicious activity they detect to our identified e-safety/safeguarding person who may then accelerate matters, if necessary, to local and/or national agencies e.g. to the Child Exploitation and Online Protection Agency (CEOP) and the Internet Watch Foundation (IWF) following agreed NSCB procedures.

2.3 FURTHER INFORMATION

2.3.1 Data Protection

We record data and information about pupils, staff and other resources. This makes us a 'data controller' and means we must adhere to a set of key principles when using data and information.

2.3.2 Data Protection Act 1998 (DPA) and GDPR 2018

2.3 Photographing Children

The definition of personal data extends to photographs of children taken by school staff or others on their behalf (e.g. professional photographers). We seek informed consent from parents in relation to the taking and using of such photographs. We do this is at the beginning of a new school year or on enrolment. Photographs are stored on secure drives and not left on devices.

2.4 Recommended Good Practice

The Data Protection Act is unlikely to apply in many cases where photographs are taken in schools and other educational institutions. Fear of breaching the provisions of the Act should not be wrongly used to stop people taking photographs or videos which provide many with much pleasure.

Where the Act does apply, a common sense approach suggests that if the photographer asks for permission to take a photograph, this will usually be enough to ensure compliance.

Photos taken for official school use may be covered by the Act and pupils and students should be advised why they are being taken.

Photos taken purely for personal use are exempt from the Act.

Examples

Personal use:

- *A parent takes a photograph of their child and some friends taking part in the school Sports Day to be put in the family photo album. These images are for personal use and the Data Protection Act does not apply.*

- *Grandparents are invited to the school nativity play and wish to video it. These images are for personal use and the Data Protection Act does not apply.*

Official school use:

- *Photographs of pupils or students are taken for building passes. These images are likely to be stored electronically with other personal data and the terms of the Act will apply.*
- *A small group of pupils are photographed during a science lesson and the photo is to be used in the school prospectus. This will be personal data but will not breach the Act as long as the children and/or their guardians are aware this is happening and the context in which the photo will be used.*

Media use:

A photograph is taken by a local newspaper of a school awards ceremony. As long as the school has agreed to this, and the children and/or their guardians are aware that photographs of those attending the ceremony may appear in the newspaper, this will not breach the Act.

2.6 Subject Access Requests

2.6.1 Data subjects (including pupils and parents) have a right of access to information held about them. In such cases they should submit a written request to the school stating clearly what they wish to access. In most cases copies of educational records must be provided with 15 working days and any other personal data within 40 working days. A child's information must only be released to a parent/guardian where such a disclosure is in the best interest of the child.

2.6.2 Usually, data should only be released to the person it relates to. In the case of young children, data can be released to parents without the child's permission. The DPA doesn't define the age at which a child is deemed to be able to take over responsibility for their own data from their parents, but the guidance suggests age 12 is usually a reasonable point. However, this may differ and cases should be considered carefully and individually.

2.6.3 Under the Act, a pupil, or someone acting on their behalf, has the right to access their personal information held by the school. This includes:

- information held on computer (or other automated means);
- information held in structured files;
- information in their educational record; and
- unstructured information, for example, held in loose correspondence

2.7 Freedom of Information Act 2000 (FOIA)

2.7.1 The FOIA provides the public with a right of access to official information. People are often unsure about the difference between FOIA and DPA. Broadly speaking, the FOI covers information on resources, aggregated information about individuals and performance information and the DPA applies to data about individuals. For example an FOIA request might include the number of staff employed, the percentage of days lost through sickness or attainment data. When considering an FOIA request for information, the DPA takes precedence. Therefore, if information requested under the FOIA could be used to derive information about specific individuals (and therefore is covered by the DPA), then the FOIA request can be refused. If in any doubt, seek advice.

2.8 Publication Schemes

2.8.1 We have adopted and we maintain a Publication Scheme. A Publication Scheme is a guide to the specific information held by a school and made available to the general public. In 2008 the ICO revised the structure of Publication Schemes and provided seven new standard headings for use by the entire public sector. They are:

- who we are and what we do;
- what we spend and how we spend it;
- what our priorities are and how we are doing;
- how we make decisions;
- our policies and procedures; and
- lists and registers / the service we offer

2.8.2 The type of information the ICO expects schools to make available (where held) under these new headings can be viewed at:

http://www.ico.org.uk/media/for-organisations/documents/1235/definition-document-chools-in-england.pdf

2.8.3 This information is available on our website.

2.9 Dealing with FOI requests

2.9.1 We are under a duty to provide advice and assistance to anyone requesting information. The enquirer is entitled to be told whether the school holds the information, except where certain exemptions apply. Requests should be dealt with within 20 working days excluding school holidays.

2.9.2 A valid FOI request should be in writing (and can include one made via an email), state the enquirer's name and correspondence address and describe the information requested. Expressions of dissatisfaction should be handled through the school's existing complaints procedure.

3 ADVICE

3.1 Staff Advice

3.1.1 Ensure a clear professional basis for all communications with students – do not give students personal telephone numbers, mobile numbers and addresses.

3.1.2 Social Networking Sites / Online Gaming

We very strongly recommend that staff do not allow access to their own personal areas or open lines of communications to students. It is very important that staff maintain professional relationships with students at all times and we feel that these may be compromised by allowing students access to personal information or photographs. However well we feel that we know students and however mature that we feel they are, it is always possible that messages may be misinterpreted by teenagers and relationships may be damaged as a result. Ensure you use appropriate privacy settings.

3.1.3 Email

It is essential that all communications with students are in connection with teaching and learning. Staff should only use their official school email address and it is recommended that students also use their school (rather than personal) email addresses when communicating with staff. The school e-mail is monitored and recorded.

3.1.4 Online publishing

It is unacceptable to publish any defamatory and/or knowingly false material about Gosforth Group, your colleagues and/or our students on social networking sites, 'blogs', 'wikis' or any other online publishing format.

3.2 Student Advice

At Gosforth Group schools lessons on the topic of online safety are built into the curriculum. These are delivered in their regular ICT and PSHCE lessons. In addition, students in Key Stages 2, 3 and 4 have assemblies on the topic. Students learn how to navigate the internet and manage information appropriately, by considering what is posted online and its reliability and validity as well as being able to identify possible hoaxes and scams and avoid falling victim to them. They are taught how to stay safe online and how to prevent challenges stemming from online use. The impact of the internet on wellbeing is also taught in IT and PSHCE lessons. Students can report any concerns via a "report abuse" button via our VLE.

The school computer network is for educational use and students should not abuse this system. When accessing the network, you must keep your password safe and you must not share your password with other people. You should not attempt to access the network area of other users or attempt to gain access to unsuitable information.

During school, staff will guide you towards appropriate materials whilst accessing the Internet. Outside of school, you should take care regarding the use of the Internet, mobile phones and social media sites:

- You should be careful about who you share your personal contact details with. This includes email addresses and mobile phone numbers.
- You should take extra care when interacting with other people in chat rooms and online. These people may not be who they say they are.
- Do not give out personal information to people you do not know very well.
- Never agree to meet anyone who you have only had contact with online.
- To help keep you safe, share the details of the people you are communicating with, online, with your parents and friends.
- Take care if accessing social networking sites such as Facebook, Twitter etc.
- Do not use social media sites to post offensive material or to make yourself vulnerable to the inappropriate actions of others.
- Avoid using mobile phones and text messages, in an inappropriate manner, which could be interpreted as cyber-bullying by the person receiving the communication.
- Take care - any photograph that you allow to be taken of you, or any image which you share online or via a mobile phone, can potentially be seen by a world audience via the Internet.

If you consider yourself, or another student, to be at risk from cyber-bullying or online safety issues, please inform an adult – either at home or school. The designated staff with responsibility for e-safety are the Safeguarding and Deputy Safeguarding Leads who can be contacted for further advice and support.

Date approved:	September 2021 ……..
Signed:	……..
Date to be reviewed:	September 2022 ……..

Gosforth Group