Greenhill School

E-Safety Policy 2015-2016

Acceptable Use Policy

Greenhill School acknowledges the educational and social benefits of ICT facilities. School members (staff and pupils) must adopt a common sense approach to the use of ICT equipment and software that gives due consideration to social and legal obligations. Inconsiderate or inappropriate use of facilities may result in disciplinary action, exclusion and possibly even legal action.

ICT facilities should normally only be used in connection with work associated with the school and not for personal or private communication. Limited and appropriate personal use is acceptable, for example during the lunch breaks or before or after the school day. Computer facilities must not be used to offend or harass, either within or outside the School. Individuals should never disrupt, interfere with or prevent anyone else using the facilities legitimately.

Certain acts are considered particularly inappropriate and will lead to action under the relevant staff or pupil Disciplinary Code and Procedures. In the case of staff, the following acts may be considered to constitute gross misconduct and could lead to dismissal:

- the use of computer facilities to offend or harass;
- the sending or relaying of sexist/racist/defamatory/indecent/obscene/pornographic/ violent/offensive e-mails, data or images;
- the accessing of sexist/racist/indecent/defamatory/obscene/pornographic/violent/ offensive material;
- the downloading, storage and distribution of such material;
- the creation of a website or screen saver of such material;
- the use of the School's ICT facilities for commercial gain or for work on behalf of others unless prior agreement has been made with the designated authority;
- the deliberate misuse of the network or networked resources, such as introducing "viruses", violating the privacy of others;
- the theft, abuse or wilful damage of computer equipment;
- the misappropriation of software belonging to another person or institution; and the sale, import and distribution of copies of software without the permission of the copyright owner.

The above list is not intended to be exhaustive, but an indication of the types of act that would be dealt with under the Disciplinary Code and Procedures.

Monitoring of Systems

The School gives notice of its ability to monitor and intercept information for the purposes of:

- establishing the existence of facts (eg to obtain evidence of business transactions);
- ascertaining compliance with regulatory or self-regulatory practices or procedures;
- ascertaining or demonstrating standards which are achieved or ought to be achieved by persons using its systems (eg for staff training or quality control);
- preventing or detecting crime;

- investigating or detecting unauthorized use of the system (eg to check that users are not downloading pornography);
- ensuring the effective operation of this system (eg to protect against “viruses”, “worms”, denial of service attacks, unauthorized access).

Monitoring is allowed under the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, made under the Regulation of Investigatory Powers Act 2000, but is also subject to the provisions of the Human Rights Act 1998 and the Data Protection Act 1998.

Authorised IT Systems Administrators require access to data held on ICT equipment or transferred over the network to ensure that networks, systems and services are operating correctly. Any information obtained in the course of such duties will be treated as confidential unless it is thought to indicate an operational problem.

Any information obtained in the course of these duties that is thought to indicate misconduct or breach of School policies will be brought to the attention of the Headteacher or his / her nominee. If deemed appropriate, further monitoring of IT and network equipment may be carried out to ensure compliance with School policies which apply to these systems. Monitoring of an individual’s ICT facilities will only be carried out when there is reason to suspect misuse and will only be carried out at the request or authorisation of the Headteacher.

Software Policy

1. Software Legal Requirements
Staff and pupils must adhere at all times to statutory law, including:

- the Theft Act 1968;
- the Copyright, Patents and Design Act 1988;
- the Computer Misuse Act 1990;
- all software within the School must be obtained legally and used in accordance with the licensing arrangement;
- school licensed software must not be copied without the express prior written consent of the ICT Department, and then only where the license permits;
- making copies of software without the permission of the copyright owner is an infringement of copyright law.

2. Software Procurement and Registration
All software must be purchased via the ICT Department. Unauthorised or nonstandard software may not be installed unless prior consent from the ICT Department is obtained. Consent is given for staff to install freeware, open source software, demonstration software and other licensed software required for teaching. The ICT Department maintains a software record log.

3. Home Use
Some software licenses allow the software to be used at home by staff. Often there will be restrictions on the use of the software for example, for use for work related purposes only. In

all such licenses the user must stop using the software when they are no longer a member of the School.

4. Viruses
Every effort must be made to ensure that computer viruses are not introduced into School. All School PCs run anti-virus software, which is updated regularly. On PCs this is an automatic process.

The creation/introduction of viruses to a computer is regarded as an unauthorised modification of computer material by the Computer Misuse Act. Such an action is an offence, which may be punished with up to 5 years imprisonment.

Information & Security – Legal Requirements

1. Information and Security Legal Requirements
Staff and Students must at all times adhere to statutory law, including:

- the Data Protection Act 1998;
- the Computer Misuse Act 1990.

2. Passwords
User passwords must not be shared. Individuals must take every precaution to ensure the privacy of their password. Individuals will be held accountable for its misuse.

Pupil passwords are set to a default, which must be changed at the first available opportunity. This is the responsibility of the pupil.

Users are required to log off or lock their workstation if they leave their systems unattended.

Unauthorised Access to Computers

Unauthorised access to computer held information is illegal. Unauthorised access to computer material is forbidden by the Computer Misuse Act 1990.

Network Services Policy

1. Email Policy
Email is a preferred primary means of communication within the School. Both staff and pupils should therefore check their mailboxes regularly. In general, email should only be used in connection to activities related to the school, but reasonable limited use is acceptable.

Authorisation from the Head of Department or Headteacher is required to access the Email account of another member of staff who is absent. Only the person's line manager will be permitted such access and the person must be informed on their return that such access has been granted.

2. Internet Policy
The School acknowledges the educational and social benefits of the use of the Internet. The internet should not be used for personal or private activities unrelated to school life, but reasonable limited use is acceptable.

3. File Storage Policy
The ICT Department provide personal file storage space for staff and pupils, and shared storage space for staff. This information is backed up daily to allow recovery of information in the events of a system failure.

Authorisation from the Head of Department or Head Teacher is required to access the personal storage area of another member of staff who is absent and the person must be informed on their return that such access has been granted.

4. Network Use
Staff, students and visitors may not connect equipment into the School's network without the agreement of the ICT Department. Any data which due to its nature, content or size, is likely to significantly affect the operation of the School network may only be transmitted subject to agreement with the ICT Department.

Equipment Policy

1. Procurement of ICT Equipment
All IT equipment must be purchased through the ICT Department.

2. Inventory/Security of Equipment
All equipment is recorded on School inventories. Any School equipment that is loaned to a member of staff is their responsibility and they must sign a loan form which must be authorised by the ICT co-ordinator or Headteacher. The individual or their department will bear the cost of replacement or repair of the equipment should it be damaged, lost or stolen in any way.

3. Equipment Change of Use/Location
Computer equipment may only be used for purposes other than its 'intended' purpose following written approval from the ICT co-ordinator or Headteacher.

4. Provision of ICT Equipment
The School aims to provide replacement staff and student PCs every five years. This is provided centrally. The School aims to provide replacement laptop/notebooks every three years.

5. Disposal of IT Equipment
The ICT Department is responsible for the disposal of all IT equipment within the School. All unwanted IT equipment must be returned to the ICT Department. All equipment that is scrapped will be disposed of in accordance with WEEE legislation.

Equipment that is no longer required by the School will be offered for sale, in the first instance to School staff or pupils. If equipment cannot be sold by the School then it can either be donated to charities/schools (if the School is satisfied that reuse of the equipment is viable), or scrapped in an environmentally sound way according to WEEE legislation.

6. Health & Safety
All equipment must be used in compliance with Health & Safety Regulations. Copies of Health & Safety Regulations are available from the School Health & Safety Officer.

Freedom of Information Policy

One of the aims of the Freedom of Information Act 2000 (which is referred to as FOIA in the rest of this document) is that public authorities, including all maintained schools, should be clear and proactive about the information they will make public.

1. How to Request Information
You can request a copy of the information you want from the contact detailed below. You can contact the school by telephone, email, fax or letter:
Email: schooladmin@greenhillsp.cardiff.sch.uk
Tel: 029 20693786
Fax: 029 20692138
Contact address: Greenhill School, Heol Brynglas, Rhiwbina, Cardiff, CF14 6UJ

2. Paying for Information
Information published on our website is free, although you may incur costs from your Internet service provider. If you don't have Internet access, you can access our website using a local library or an Internet café. If your request for copies of information requires considerable photocopying, printing or large postage charges, or is for a priced item such as some printed publications or videos we will let you know the cost before fulfilling your request.

Data Protection Policy

The School is required to process relevant personal data regarding pupils and their parents/carers and shall take all reasonable steps to do so in accordance with this Policy. Processing may include obtaining, recording, holding, disclosing, destroying or otherwise using data. In this Policy any reference to pupils includes current, past or prospective pupils.

All school staff will endeavour to ensure that all personal data is processed in compliance with this Policy and the Principles of the Data Protection Act 1998, ie that all data is:

- fairly and lawfully processed;
- processed for a lawful purpose;
- adequate, relevant and not excessive;
- accurate and up to date;
- not kept for longer than necessary;
- processed in accordance with the data subject's rights;
- secure;

- not transferred to other countries without adequate protection.

1. Personal Data

Personal data covers both facts and opinions about an individual. The School may process a wide range of personal data of pupils or their parents/carers as part of its operation. This personal data may include (but is not limited to);

- names and addresses, bank details, academic, disciplinary, admissions;and
- attendance records, references, examination scripts and marks.

2. Processing Of Personal Data

Consent may be required for the processing of personal data unless the processing is necessary for the School to undertake its obligations to pupils and their parents or guardians. Any information which falls under the definition of personal data, and is not otherwise exempt, will remain confidential and will only be disclosed to third parties with the consent of the appropriate individual or under the terms of this Policy.

3. Sensitive Personal Data

The School may, from time to time, be required to process sensitive personal data regarding a pupil, their parents or guardians. Sensitive personal data includes medical information and data relating to religion, race, or criminal records and proceedings. Where sensitive personal data is processed by the School, the explicit consent of the appropriate individual will generally be required in writing.

4. Rights Of Access

Individuals have a right of access to information held by the School. Any individual wishing to access their personal data should put their request in writing to the Headteacher. [Please note that the School may charge an administration fee for providing this information.]

You should be aware that certain data is exempt from the right of access under the Data Protection Act. This may include information which identifies other individuals, information which the School reasonably believes is likely to cause damage or distress, or information which is subject to legal professional privilege. The School is also not required to disclose any pupil examination scripts.

The School will also treat as confidential any reference given by the School for the purpose of the education, training or employment, or prospective education, training or employment of any pupil or member of staff.

5. Who's Rights

The rights under the Data Protection Act are the individual's to whom the data relates. However, in most cases, the School will rely on parental/carer consent to process data relating to pupils. The School will only grant the pupil direct access to their personal data if in the School's reasonable belief the pupil understands the nature of the request.

6. Exemptions

Certain data is exempted from the provisions of the Data Protection Act which includes the following:

- the prevention or detection of crime;
- where the processing is necessary to exercise a right or obligation conferred or imposed by law upon the School.

The above are examples only of some of the exemptions under the Act.

7. Disclosure of Information

The School may receive requests from third parties to disclose personal data it holds about pupils, their parents or guardians. The School confirms that it will not generally disclose information unless the individual has given their consent or one of the specific exemptions under the Data Protection Act applies. However the School does intend to disclose such data as is necessary to third parties for the following purposes:

- to give confidential references relating to a pupil to any educational institution which it is proposed that the pupil may attend;
- to publish the results of public examinations or other achievements of pupils of the school;
- to disclose details of a pupil's medical condition where it is in the pupil's interests to do so, for example for medical advice, insurance purposes or to organisers of school trips.

Where the School receives a disclosure request from a third party it will take reasonable steps to verify the identity of that third party before making any disclosure.

8. Use of Personal Information By The School

The School will, from time to time, make use of personal data relating to pupils, their parents/carers in the following ways:

- to make use of photographic images of pupils in School publications and on the School website. However the School will not publish photographs of individual pupils with their names on the School website without the express agreement of the appropriate individual. The school will not publish photographs of Looked After Children without the consent of Children's Services;
- for fundraising, marketing or promotional purposes.

9. Accuracy

The School will endeavour to ensure that all personal data held in relation to an individual is accurate. Individuals must notify the Headteacher about any changes to information held about them. An individual has the right to request that inaccurate information about them is erased or corrected.

10. Security

The School will take reasonable steps to ensure that members of staff will only have access to personal data relating to pupils, their parents/carers where it is absolutely necessary. All staff will be made aware of this policy and their duties under the Data Protection Act. The School will ensure that all personal information is held securely and is not accessible to unauthorised

persons. Where staff are transporting personal information about a pupil or parent/carer (eg on a removable drive) they must ensure that files are encrypted.

11. Enforcement
If an individual believes that the School has not complied with this Policy or acted otherwise than in accordance with the Data Protection Act, they are asked first to contact the Headteacher. If they wish to take further action, they should ask for sight of the School's Complaints Procedure.

Photo & Images Policy

1. Child Protection Issues
Risks occur when individual children can be identified in photographs. Wherever the school finds images being used inappropriately, the matter will be reported to the LA in the same way as any other child protection issue.

2. Data Protection Act
Photographs and video images of pupils and staff are classed as personal data under the terms of the Data Protection Act 1998. Therefore, using such images requires the consent of either the individual concerned, or in the case of children, their parent/carer or, in the case of Looked After Children,
Children's Services. The school will not display images of pupils or staff on websites, in publications or in a public place, without such consent and the reason for using a person's image and how it will be used must be made clear. However, if images are taken at an event attended by large crowds, this is regarded as a public area, so permission is not required from everyone in a crowd shot. Individuals in the foreground are also considered to be in a public area, but if any individuals are identifiable in the photograph, consent is needed.

3. Appropriate Use of Images
The problem of identification can be avoided by only using group or whole class shots, or by ensuring faces are out of focus or partly or wholly turned away from the camera. However, this will produce very dull photographs. The following rules will apply:

- if the child is named, avoid using their photograph;
- if a photograph is used, avoid naming the child;
- only use photographs of children in suitable dress. Children in swimming costumes are not to be photographed. Where children are photographed in PE kit, the content of the photograph should focus on the activity and avoid full face or full body shots;
- children subject to a court order should not be used in a photograph;
- images must be stored securely and only used by those authorised to do so;
- the Headteacher should consider whether to destroy images after use;
- photographs of children should not be used after they have left the school;
- parental consent for the use of full face or full body shots should be sought.

4. Websites
There is greater risk of misuse of images on the Internet because of the lack of control over who might see the image. Although the rules are the same as for any other type of image, it is

essential that parental/carer (and Children Services for Looked After Children) consent has been gained for any image of a child that is put on websites. Similarly the consent of any adult must be gained prior to putting their image on the website. All consents must be in writing on the agreed consent form.

5. Newspapers

Newspapers tend to want to put the names of pupils in photographs. As long as parental consent is gained and it is made clear that the photograph will be published in a newspaper, this is not a cause for concern. There are already strict guidelines for newspapers through the Press Complaints Commissions' Code of Practice. Specifically, no child under 16 may be interviewed about his/her welfare and no child may be interviewed while at school without permission. There is no breach of the Data Protection Act by simply passing on a child's name as long as parental consent has been gained.

6. Filming School Events

Parents and spectators may want to photograph or video an event at school, such as a sports day or an arts performance. This is not a cause for concern providing parents/carers are fully aware of our expectations. The process is as follows:

- we do not seek the permission of parents for images to be taken at any specific event;
- any parent wanting to photograph or film an event must tell the Headteacher. Common practice will be that permission will be given to parents and relatives known to the school but there is an implicit understanding that any image created will be solely for the use of parent or relative taking the image;
- any parent who has a concern regarding the taking of images at an event should contact the Headteacher immediately.

7. Parental Consent

We will also request written parental permission for taking photographs of their child as part of the registration process when a child starts school. These consent forms will be retained in the school office. It is the responsibility of the parents/carer to alter any details on the consent form.

REVIEW DATE:

SIGNED: _____

Jayne Cowan – Chair of Governors