Bancroft's School

ON-LINE SAFETY POLICY

RESPONSIBILITY

The Designated Safeguarding Lead (DSL) has been designated as responsible for pupil safety and security policies related to the Internet and electronic communications.

The DSL along with the IT Manager ensure that policies are implemented and that regular monitoring takes place. All staff, including temporary and student teachers, are made aware of school ICT policies.

All members of staff and pupils should be encouraged to use computers and the Internet responsibly and to understand the consequences their actions could have on themselves and others.

SUPERVISION

Pupils at Bancroft's are made aware that, a teacher, or responsible adult, may be supervising indirectly, but still be aware of pupils' access and monitoring their use.

When direct supervision by school staff is not possible, those with responsibility for pupils are aware of the school's policies on Internet Safety.

For example, pupils on school organised work placement schemes, exchanges and training courses should not be allowed to have unsupervised, unfiltered Internet access.

When a pupil enrols at Bancroft's they are asked to sign the E-citizen charter, parents are sent a copy and encouraged to discuss this with their children.

E-CITIZEN CHARTER & ACCEPTABLE USE POLICY

Pupils must sign an E-Citizen Charter

Such an agreement makes everyone aware of their responsibilities when using the Internet. Parents are sent a copy of the E-Citizen charter.

USE OF THE INTERNET

The Internet can be a rich educational resource, providing access to millions of pages of information. However, much of the Internet is unorganised and unregulated and many sites contain information, which is inaccurate, dangerous, illegal or pornographic.

Bancroft's tries to ensure that pupils do not have bad experiences when using the Internet or other forms of electronic communication and that parents have confidence that Bancroft's are using 'all due diligence' to protect their children. Above all, we want to avoid pupils being exposed to offensive materials – pornographic, violent, or racist.

CHILD PROTECTION

The most serious risk to pupils involves the possibility of someone being hurt, exploited or abused as a result of personal information being posted online. Online pictures, names, addresses, or age can be used to trace, contact and meet a pupil with the intention of causing harm. The internet can also be a source of peer-on-peer abuse and all pupils receive guidance on how to respond to cyber-bullying if it occurs. Further information on our approach to this can be found in the Anti-Bullying Policy.

INTERNET FILTERING

The statutory guidance makes clear the need for schools to ensure that children are safe from terrorist and extremist material when accessing the internet in schools, this includes potentially harmful and inappropriate online material. The school has in place filtering software to prevent access to terrorist and extremist websites and identify the use of search engines to search any terms which may be associated with such organisations.

As with other online risks of harm, every teacher needs to be aware of the risks posed by the online activity of extremist and terrorist groups and they must raise any concerns about pupil on-line activity with the DSL.

MOBILE TECHNOLOGY

The Bursar's office has a number of mobile phones that are available, on application, for members of staff who require them for School activities.

The following school policy regarding pupil use of mobiles phones will apply:

- All pupils who bring mobile phones and tablets to school should leave them locked in their locker, for example when going to games/PE, or on their person. These devices remain the sole responsibility of the pupil. Tutors are asked to remind their pupils that expensive devices left around have a habit of going missing. There is a mobile phone use policy which details which year groups may use their phones around school and where. This policy is printed in the school calendar.

- The obtrusive use of a mobile phone, without staff permission, by a pupil is forbidden in any lesson. Obviously staff should use their judgement as to whether the use of such is obtrusive or otherwise. For example recording homework on a mobile phone maybe entirely appropriate.

- Pupils and staff may use the Bancroft's School Wi Fi service by logging in once upon entry to the building. This Wi Fi is then subject to the school's filters and monitored

by the School's IT staff. Any attempts to gain access to harmful or inappropriate websites is flagged to the Senior Deputy Head and DSL.

Appendix One

IT acceptable use policy from the staff employment manual

1 **Introduction:** This policy sets out the requirements with which you must comply when using the School's IT and when otherwise using IT in connection with your job including:

1.1 the School's email and internet services;

1.2 telephones and faxes;

1.3 the use of mobile technology on School premises or otherwise in the course of your employment (including 3G / 4G or Bluetooth or other wireless technologies), whether using a school or a personal device; and

1.4 any hardware (such as laptops, printers or mobile phones) or software provided by, or made available by, the School.

This policy also applies to your use of IT off school premises if the use involves Personal Information of any member of the School community or where the culture or reputation of the School are put at risk.

2 **Failure to comply:** Failure to comply will constitute a disciplinary offence and will be dealt with under the School's disciplinary procedure.

3 **Property:** You should treat any property belonging to the School with respect and reasonable care and report any faults or breakages immediately to the Bursar. You should not use the School's computers or other IT resources unless you are competent to do so and should ask for training if you need it.

4 **Viruses and other malicious code:** You should be aware of the potential damage that can be caused by computer viruses and other malicious code. You must not use, introduce or operate any hardware, programmes or data (including computer games) or open suspicious emails without permission from the IT department.

5 **Passwords:** Passwords should be long, for example, you could use a song lyric or a memorable phrase plus a number. Do not choose a password which is so complex that it's difficult to remember without writing it down. Your password should not be disclosed to anyone else. In addition:

5.1 Your password should be difficult to guess, for example, you could base your password on something memorable that no-one else would know. You should not use information which other people might know, or be able to find out, such as your address or your birthday.

5.2 You must not use a password which is used for another account. For example, you must not use your password for your private email address or online services for any school account.

5.3 Passwords (and any other security credential you are issued with such as a key fob or USB drive) must be kept secure and confidential and must not be shared with, or given to, anyone else. Passwords should not be written down.

6 **Leaving workstations:** If you leave your workstation for any period of time you should take appropriate action and, in particular, you should lock your screen to prevent access.

7 **Concerns**: You have a duty to report any concerns about the use of IT at the School to the Senior Deputy Head and/or Designated Safeguarding Lead as appropriate; for example, if you have a concern about IT security or pupils accessing inappropriate material.

8 **Other policies**: This policy should be read alongside the following:

8.1 Code of Conduct;

8.2 Data Protection policy for Staff;

8.3 Information Security policy; and

8.4 Acceptable Use policy for Pupils.

Internet

9 **Downloading:** Downloading of any programme or file which is not specifically related to your job is strictly prohibited.

10 **Personal use:** The School permits the incidental use of the internet so long as it is kept to a minimum and takes place substantially out of normal working hours. Use must not interfere with your work commitments (or those of others). Personal use is a privilege and not a right. If the School discovers that excessive periods of time have been spent on the internet provided by the School or it has been used for inappropriate purposes (as described in section 11 below), either in or outside working hours, disciplinary action may be taken and internet access may be withdrawn without notice at the discretion of the Head.

11 **Unsuitable material:** Viewing, retrieving or downloading of pornographic, terrorist or extremist material, or any other material which the School believes is unsuitable is strictly prohibited and constitutes gross misconduct. This includes such use at any time on the School's network, or via 3G or 4G when on School premises or otherwise in the course of your employment and whether or not on a School or personal device. Internet access may be withdrawn without notice at the discretion of the Head whilst allegations of unsuitable use are investigated by the School.

12 **Location services**: The use of location services represents a risk to the personal safety of those within the School community, the School's security and its reputation. The use of any website or application, whether on a School or personal device, with the capability of publicly identifying the user's location while on School premises or otherwise in the course of employment is strictly prohibited at all times.

13 **Contracts:** You are not permitted to enter into any contract or subscription on the internet (including through an App) on behalf the School, without specific permission from the Bursar. This applies both to "free" and paid for contracts, subscriptions and Apps.

Email

14 **Personal use:** The School permits the incidental use of its email systems to send personal emails as long as such use is kept to a minimum and takes place substantially out of normal working hours. Personal emails should be labelled "personal" in the subject header. Use must not interfere with your work commitments (or those of others). Personal use is a privilege and not a right. The School may monitor your use of the email system and staff should advise those they communicate with that such emails may be monitored. If the School discovers that you have breached these requirements, disciplinary action may be taken.

15 **Status:** Email should be treated in the same way as any other form of written communication. Anything that is written in an email is treated in the same way as any form of writing. You should not include anything in an email which is not appropriate to be published generally.

16 **Inappropriate use:** Any email message which is abusive, discriminatory on grounds of sex, marital or civil partnership status, age, race, disability, sexual orientation or religious belief (or otherwise contrary to our equal opportunities policy), or defamatory is not permitted. Use of the email system in this way constitutes gross misconduct. The School will take no responsibility for any offence caused by you as a result of downloading, viewing or forwarding inappropriate emails.

17 **Legal proceedings:** You should be aware that emails are disclosable as evidence in court proceedings and even if they are deleted, a copy may exist on a back-up system or other storage area.

18 **Jokes:** Trivial messages and jokes should not be sent or forwarded to the email system. They could cause the School's IT system to suffer delays and / or damage or could cause offence.

19 **Contracts:** Contractual commitments via an email correspondence are not allowed without the prior authorisation of the Bursar.

20 **Disclaimer:** All correspondence by email should contain the School's disclaimer.

21 **Data protection disclosures:** Subject to a number of limited exceptions, potentially all information about an individual may be disclosed should that individual make a subject access request under data protection legislation. There is no exemption for embarrassing information (for example, an exchange of emails containing gossip about the individual will usually be disclosable). **Staff must be aware that anything they put in an email is potentially disclosable.**

Monitoring

22 The School regularly monitors and accesses its IT system for purposes connected with the operation of the School. The School IT system includes any hardware, software, email account, computer, device or telephone provided by the School or used for School business. The School may also monitor staff use of the School telephone system and voicemail messages. Staff should be aware that the School may monitor the contents of a communication (such as the contents of an email).

23 The purposes of such monitoring and accessing include:

23.1.1 to help the School with its day to day operations. For example, if a member of staff is on holiday or is off sick, their email account may be monitored in case any urgent emails are received; and

23.1.2 to check staff compliance with the School's policies and procedures and to help the School fulfil its legal obligations. For example, to investigate allegations that a member of staff has been using their email account to send abusive or inappropriate messages.

24 Monitoring may be carried out on a random basis and it may be carried out in response to a specific incident or concern.

25 The School also uses software which automatically monitors the School IT system (for example, it would raise an alert if a member of Staff visited a blocked website or sent an email containing an inappropriate word or phrase).

The monitoring is carried out by the IT Department. If anything of concern is revealed as a result of such monitoring then this information may be shared with the Senior Deputy Head and/or DSL as appropriate and this may result in disciplinary action. In exceptional circumstances concerns will need to be referred to external agencies such as the Police.

Appendix Two – Bancroft's School Responsible E-Citizen Charter

Bancroft's School recognises that the use of ICT (information and communication technology) can enhance the learning experience of our students. However we also recognise that the use of ICT can introduce some risk factors. In order to help our students manage those risks we have a program of education for students and staff, and we also provide information for parents. To help reinforce the guidelines for safe responsible use of ICT we have produced the following agreement which we are asking students to sign.

As a student at Bancroft's School I agree to the following when at school or engaged in school activities or on school trips:

1) I will be careful not to post personal information about myself or others on to public areas of the Internet.

2) I will ensure that before I send or post any photo or video that the content is not inappropriate and that I have the permission of those whose image is included to send or post the content. If it is shot on private property I will also make sure that the owners of the property do not prohibit photography or filming.

3) I will consider the feelings of others before I post, send or forward any information or comments about any person and will not post, send or forward any information or comment if I believe it may cause upset or distress to anyone.

4) When using school equipment I will do my best to use it in a way that helps to maintain it in good working order. If I discover that a piece of equipment is broken or malfunctioning in any way I will report it to a member of staff so that it can be repaired. I will leave equipment in a tidy and clean state.

5) I will avoid the technical and legal problems that unauthorised software access causes by not installing, attempting to install or reconfiguring any software / hardware on any school equipment. I will only use the software provided by Bancroft's School when using school equipment.

6) I will help to maintain the security of the school ICT systems by only using the account(s) that I have been authorised to use, by not attempting to bypass any settings and by not helping anyone to gain unauthorised access to any school system or third party systems.

7) I will help to maximise the availability of school ICT equipment by only using school equipment and my authorised account(s) / school email addresses for tasks related to coursework, homework or co-curricular activities organised by the school.

I understand that by using the school ICT equipment I am agreeing to abide by the above conditions. I understand that the school retains the right to retain and use copies of all data that is created, stored or transmitted using equipment it owns. I understand that if I contravene the above guidelines that some form of disciplinary action may be taken. This could include having my computer access suspended and my parents being notified. The

appropriate authorities may be notified if illegal activity has taken place. I also understand that the school will notify my parents of any concerns about aspects of my online behaviour that affects the well-being of myself or others. I also understand that, when using services provided by a third party, I will need to abide by the terms and conditions that they set.

Responsible E-Citizen Charter FAQs
If you have any further questions please contact ICT department or the Senior Deputy Head.

1 Does the E-Citizen Charter refer to my computer use out of school?
The E-Citizen charter refers to what you do while at school, on a school trip, or using school equipment via a remote link. However we would like you to consider points 1 to 3 whenever you are using ICT equipment as these points are concerned with the wellbeing of you and others.

2 How does the warning about posting personal information apply to computer use at school?
You may not use school computers to post personal information about yourself or others which could put yourself or others at risk. For example if accessing Fantasy Football for Maths you should use a nickname.

Safeguarding personal information is recommended at home, too, but there the matter is the responsibility of yourself and your parents. The ThinkUKnow website gives you advice about this. www.thinkuknow.co.uk

Please be aware that some online services reveal your GPS location, which can enable others to stalk you. Also photos taken on many smart phones contain GPS location information; this function should generally be switched off if you are posting photos online.

3. How do I know if a property owner has given permission for photography/video?
Most establishments will display signs if photography/video is forbidden.eg museums, places of worship. If in doubt ask the teacher who is in charge of the trip.

4. Bancroft's is private property….can I take photos/videos?
You should not bring valuables such as cameras to school, however it is likely that your phone has a camera facility. This should be locked in your locker during lesson time.
There may be occasions when a teacher allows you to bring a phone/camera into the classroom. **You must have the express permission of the teacher to take a photo/video in a lesson**. All those in the image must give their consent.

When not in lessons students may take photographs/videos providing the content is appropriate. You must have the consent of all those in the image. Students must abide by the Anti-Bullying Policy. Using photographic material of any kind to bully, harass or intimidate others will not be tolerated and will constitute a serious breach of discipline.
Students must be aware that staff in charge may apply restrictions on taking images during some activities such as plays and concerts.

5. Is it practical to obtain the permission of everyone featured in a photo/video?
You should confirm that the main characters, usually your friends, (not people in the background in a large crowd), are willing to be in a photo/video. Respect the wishes of anybody who does not want you to photograph or video them.

The Bancroft's E-Citizen Charter applies only to images of Bancroftians, at school or engaged on school activities off site, and any images posted on the Bancroft's system. It is good practice to respect privacy in other contexts, too, but this is your own responsibility.

6. Will I be causing distress if I express views on a controversial subject?
The E-Citizen Charter does not prohibit the expression of views on current affairs topics. However controversial and sensitive issues are best debated in a classroom where a teacher chairs the discussion and a range of views can be put forward.

The E-Citizen Charter prohibits causing upset or distress by bullying. This is made clear in our Anti Bullying Policy (in the calendar).

7. What does the school do with the data I have created, stored and transmitted?
Files that students create in their personal area are deleted 6 months after they leave. The data would also be held on backup tape for at least a year. Internet browsing histories would be retained for longer but only in the form of an offline archive.

Some examples of students work may be retained for ICT teaching purposes or to display on open days. In the case of data, generally photos, that students submit to staff to go onto the students' shared drives, they will remain until the member of staff who placed them there removes them.

8. What do you mean by services provided by third parties?
Third parties services are, for example, Microsoft's Live@Edu eMail and Office Live. All senior school students have a Microsoft Live@Edu email account. When you are accessing these hosted Microsoft services you will have to agree to the service terms and conditions (in addition to the school's E-Citizen Charter.)