



**BARCLAY
ACADEMY**
LIBERTAS PER CULTUM

Online Safety Policy

September 2022



Online Safety Policy

Contents:

1. Context within the school
2. Managing the Internet Safely
3. Policy: Use of digital and video images
4. Policy: Managing the network and Equipment
5. Education and Training
6. Policy: How will Infringements be handled?
7. Guidance: What do we do if?
8. How will staff and students be informed of these procedures?
9. Appendices

1. Context: Online Safety Policy September 2022

Barclay Academy's top priority is to ensure that all its pupils are safe and that they work in a safe, happy and caring environment. Ensuring that our pupils engage with technology in a safe manner is part of that overall responsibility.

2. Managing the Internet Safely

Technical and Infrastructure approaches

Barclay Academy:

- Has the educational filtered secure broadband connectivity through the LGfL and so connects to the 'private' National Education Network;
- Uses the LGfL filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc. All changes to the filtering policy is logged and only available to staff with the approved 'web filtering management' status;
- Uses USO user-level filtering where relevant, thereby closing down or opening up options appropriate to the age / stage of the students;
- Blocks all Chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform;

- Has blocked pupil access to music download or shopping sites – except those approved for educational purposes at a regional or national level, such as Audio Network;
- Uses security time-outs on Internet access where practicable / useful;
- Provides staff with an email account for their professional use, *Barclay Academy / Future academies email* and makes clear personal email should be through a separate account;
- *Uses teacher 'remote' management control tools for controlling workstations / viewing users / setting-up applications and Internet web sites, where useful;*
- *Has additional local network auditing software installed;*
- Works in partnership with the LGfL to ensure any concerns about the system are communicated so that systems remain robust and protect students;
- Ensures the Systems Administrator / network manager is up-to-date with LGfL services and policies / requires the Technical Support Provider to be up-to-date with LGfL services and policies;

3. Policy: Use of digital and video images

In Barclay Academy:

- We gain parental / carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter / son joins the school;
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials / DVDs;
- Staff sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones / personal equipment for taking pictures of pupils;
- The school blocks/filter access to social networking sites or newsgroups unless there is a specific approved educational purpose;
- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identify of others and their location, such as house number, street name or school. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.
- Pupils should not be using mobile phones in school. No child should make any digital recording (image or sound) in school using any personal equipment, without express permission from senior staff.
- Parents are advised that any images they take in school should not be shared via any public source and should not identify any child by name. The school reserves the right to instruct parents to take no photographs or video for selected events.

Website:

- The school web site complies with the DfE's guidelines for publications;
- The point of contact on the web site is the school address, telephone number and we use a general email contact address, e.g. admin@barclay.futureacademies.org. Home information or individual e-mail identities will not be published;
- Photographs published on the web do not have full names attached;
- We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website;
- We expect teachers using school approved blogs or wikis to password protect them and run from the school website.

4. Policy: Managing the network and Equipment

Using the school network, equipment and data safely: general guidance

The computer system / network is owned by the school and is made available to students to further their education and to staff to enhance their professional activities including teaching, research, administration and management.

The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet or email activity on the network.

To ensure the network is used safely Barclay Academy:

- Ensures staff read and sign that they have understood the school's online safety Policy. Following this, they are set-up with Internet, email access and network access. Online access to service is through a unique, audited username and password. We also provide a different username to all staff and use the same username and password for pupils for access to our school's network;
- We provide pupils with an individual network log-in username.
- Makes it clear that staff and pupils must always keep their password private, must not share it with others and must not leave it where others can find. ;
- Makes clear that no one should log on as another user and makes clear that pupils should never be allowed to log-on or use teacher and staff logins as these have far less security restrictions and inappropriate use could damage files or the network;
- Has set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas;
- Requires all users to always log off when they have finished working or are leaving the computer unattended;
- Where a user finds a logged-on machine, we require them to always log-off and then log-on again as themselves.
- Our wireless network has been secured to industry standard Enterprise security level /appropriate standards suitable for educational use.
-

5. Education and Training

Barclay Academy:

- Fosters a 'No Blame' environment that encourages pupils to tell a teacher / responsible adult immediately if they encounter any material that makes them feel uncomfortable;
- Teaches pupils and informs staff what to do if they find inappropriate web material i.e. to switch off monitor and report the URL to the teacher or System Manager.
- Ensures pupils and staff know what to do if there is a cyber-bullying incident;
- Ensures all pupils know how to report any abuse;
- Has a clear, progressive online safety education programme throughout all Key Stages, built on Local Authority / national guidance. Pupils are taught a range of skills and behaviours appropriate to their age and experience, such as:
 - to STOP and THINK before they CLICK
 - to discriminate between fact, fiction and opinion;
 - to develop a range of strategies to validate and verify information before accepting its accuracy;
 - to skim and scan information;

- to be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be;
 - to know how to narrow down or refine a search;
 - to understand how search engines work and to understand that this affects the results they see at the top of the listings;
 - to understand 'Netiquette' behaviour when using an online environment / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private;
 - to understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
 - to understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments;
 - to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings;
 - to understand why they must not post pictures or videos of others without their permission;
 - to know not to download any files – such as music files - without permission;
 - to have strategies for dealing with receipt of inappropriate materials;
 - to understand why and how some people will 'groom' young people for sexual reasons;
 - understand that different systems have different levels of security which will require them to act in different ways;
 - provide strategies for identifying less secure systems/ websites and for self-managing risk in scenarios where systems are not locked down or have variable security settings.
- Ensures that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must observe and respect copyright / intellectual property rights;
 - Ensures staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection;
 - Makes training available annually to staff on the online safety education program;
 - Runs a rolling programme of advice, guidance and training for parents, including:
 - Information leaflets; in school newsletters; on the school web site;
 - Access to resources, information and training on National Online Safety
 - suggestions for safe Internet use at home;
 - provision of information about national support sites for parents;

6. Policy: How will infringements be handled?

Whenever a student or staff member infringes the Online Safety Policy, the final decision on the level of sanction will be at the discretion of the school management and will reflect the school's behaviour and disciplinary procedures.

The following are provided as **exemplification** only:

STUDENT	
Category A infringements	Possible Sanctions:
<ul style="list-style-type: none"> ● Use of non-educational sites during lessons ● Unauthorised use of email 	Refer to class teacher / Head of Year

<ul style="list-style-type: none"> • Unauthorised use of mobile phone (or other new technologies) in lessons e.g. to send texts to friends • Use of unauthorised instant messaging / social networking sites 	Escalate to: senior manager
<p style="text-align: center;">Category B infringements</p>	<p style="text-align: center;">Possible Sanctions:</p>
<ul style="list-style-type: none"> • Continued use of non-educational sites during lessons after being warned • Continued unauthorised use of email after being warned • Continued unauthorised use of mobile phone (or other new technologies) after being warned • Continued use of unauthorised instant messaging / chatrooms, social networking sites, NewsGroups • Use of Filesharing software • Trying to buy items online • Accidentally corrupting or destroying others' data without notifying a member of staff of it • Accidentally accessing offensive material and not logging off or notifying a member of staff of it 	<p>Refer to Class teacher/ senior leader</p> <p>Escalate to:</p> <p>removal of Internet access rights for a period / contact with parent</p>
STUDENT	
<p style="text-align: center;">Category C infringements</p>	<p style="text-align: center;">Possible Sanctions:</p>
<ul style="list-style-type: none"> • Deliberately corrupting or destroying someone's data, violating privacy of others or posts inappropriate messages, videos or images on a social networking site. • Sending an email or MSN message that is regarded as harassment or of a bullying nature (one-off) • Trying to access offensive or pornographic material (one-off) • Purchasing or ordering of items online • Transmission of commercial or advertising material 	<p>Refer to Class teacher / Head of Year / Principal / removal of Internet and/or Learning Platform access rights for a period</p> <p>Escalate to: contact with parents / removal of equipment</p> <p>Other safeguarding actions if inappropriate web material is accessed: Ensure appropriate technical support filters the site</p>
<p style="text-align: center;">Category D infringements</p>	<p style="text-align: center;">Possible Sanctions:</p>
<ul style="list-style-type: none"> • Continued sending of emails or MSN messages regarded as harassment or of a bullying nature after being warned • Deliberately creating accessing, downloading or disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent • Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of GDPR and data protection legislation. • Bringing the school name into disrepute 	<p>Refer to Principal / Contact with parents</p> <p>Other possible safeguarding actions:</p> <ul style="list-style-type: none"> • Secure and preserve any evidence • Inform the sender's e-mail service provider. • Liaise with relevant service providers/ instigators of the offending material to remove • Report to Police / CEOP where child abuse or illegal activity is suspected

STAFF	
Category A infringements (Misconduct)	Possible Sanctions:
<ul style="list-style-type: none"> • Excessive use of Internet for personal activities not related to professional development e.g. online shopping, personal email, instant messaging etc. • Use of personal data storage media (e.g. USB memory sticks) without considering access and appropriateness of any files stored. • Not implementing appropriate safeguarding procedures. • Any behaviour on the World Wide Web that compromises the staff members professional standing in the school and community. • Misuse of first level data security, e.g. wrongful use of passwords. • Breaching copyright or license e.g. installing unlicensed software on network. 	<p>Referred to line manager / Principal</p> <p>Escalate to:</p> <p><i>Warning given</i></p>
Category B infringements (Gross Misconduct)	Possible Sanctions:
<ul style="list-style-type: none"> • Serious misuse of, or deliberate damage to, any school / Council computer hardware or software; • Any deliberate attempt to breach data protection or computer security rules; • Deliberately creating ,accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent; • Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988; • Bringing the school name into disrepute 	<p>Referred to Principal / Governors;</p> <p>Other safeguarding actions:</p> <ul style="list-style-type: none"> ▪ Remove the PC to a secure place to ensure that there is no further access to the PC or laptop. ▪ Instigate an audit of all ICT equipment by an outside agency, such as the schools ICT managed service providers - to ensure there is no risk of pupils accessing inappropriate materials in the school. ▪ Identify the precise details of the material. <p><i>Escalate to:</i></p> <p><i>report to LA /LSCB, Personnel, Human resource.</i></p> <p>Report to Police / CEOP where child abuse or illegal activity is suspected. ,</p>

If a member of staff commits an exceptionally serious act of gross misconduct

The member of staff should be instantly suspended. Normally though, there will be an investigation before disciplinary action is taken for any alleged offence. As part of that the member of staff will be asked to explain their actions and these will be considered before any disciplinary action is taken.

Schools are likely to involve external support agencies as part of these investigations e.g. an ICT technical support service to investigate equipment and data evidence.

Child abuse images found

In the case of Child abuse images being found, the member of staff should be **immediately suspended** and the Police should be called.

Anyone may report any inappropriate or potentially illegal activity or abuse with or towards a child online to the Child Exploitation and Online Protection (CEOP):

http://www.ceop.gov.uk/reporting_abuse.html

<http://www.iwf.org.uk>

7. Guidance: What do we do if?

An inappropriate website is accessed unintentionally in school by a teacher or child.

1. Play the situation down; don't make it into a drama.
2. Report to the Principal/online safety officer and decide whether to inform parents of any children who viewed the site.
3. Inform the school technicians and ensure the site is filtered (LGfL schools report to: **webalerts@synetrix.com**).
4. Inform the LA if the filtering service is provided via an LA/RBC.

An inappropriate website is accessed intentionally by a child.

1. Refer to the acceptable use policy that was signed by the child, and apply agreed sanctions.
2. Notify the parents of the child.
3. Inform the school technicians and ensure the site is filtered if need be.
4. Inform the LA if the filtering service is provided via an LA/RBC.

An adult uses School IT equipment inappropriately.

1. Ensure you have a colleague with you, do not view the misuse alone.
2. Report the misuse immediately to the Principal and ensure that there is no further access to the PC or laptop.
3. If the material is offensive but not illegal, the head teacher should then:
 - Remove the PC to a secure place.
 - Instigate an audit of all ICT equipment by the schools ICT managed service providers to ensure there is no risk of pupils accessing inappropriate materials in the school.
 - Identify the precise details of the material.
 - Take appropriate disciplinary action (contact Human Resources).
 - Inform governors of the incident.
4. In an extreme case where the material is of an illegal nature:
 - Contact the local police or High Tech Crime Unit and follow their advice.
 - If requested to remove the PC to a secure place and document what you have done.

A bullying incident directed at a child occurs through email or mobile phone technology, either inside or outside of school time.

1. Advise the child not to respond to the message.
2. Refer to relevant policies including online safety and anti-bullying and apply appropriate sanctions.
3. Secure and preserve any evidence.
4. Notify parents of the children involved.
5. Consider delivering a parent workshop for the school community.
6. Inform the police if necessary.

Malicious or threatening comments are posted on an Internet site about a pupil or member of staff.

1. Inform and request the comments be removed if the site is administered externally.
2. Secure and preserve any evidence.

3. Send all the evidence to CEOP at www.ceop.gov.uk/contact_us.html.
4. Endeavour to trace the origin and inform police as appropriate.

The school may wish to consider delivering a parent workshop for the school community

You are concerned that a child's safety is at risk because you suspect someone is using communication technologies (such as social networking sites) to make inappropriate contact with the child

1. Report to and discuss with the named child protection officer in school and contact parents.
2. Advise the child on how to terminate the communication and save all evidence.
3. Contact CEOP <http://www.ceop.gov.uk/>
4. Consider the involvement police and social services.
5. Consider delivering a parent workshop for the school community.

All of the above incidences must be reported immediately to the Principal and Designated Safeguarding Lead.

Children should be confident in a no-blame culture when it comes to reporting inappropriate incidents involving the internet or mobile technology: they must be able to do this without fear.

8. How will staff and students be informed of these procedures?
--

- They will be fully explained and included within the school's online safety / Acceptable Use Policy. All staff will be required to sign the school's online safety acceptable use agreement form;
- Pupils will be taught about responsible and acceptable use and given strategies to deal with incidents so they can develop 'safe behaviours'. Pupils will sign an age appropriate online safety / acceptable use agreement form;
- The school's online safety policy will be made available and explained to parents, and parents will sign an acceptance form when their child starts at the school.
- Information on reporting abuse / bullying etc will be made available by the school for pupils, staff and parents.
- Staff are issued with the 'What to do if?' guide on e-safety issues, (see LGFL safety site)

9. Appendices

9.1. Acceptable use policy

 BARCLAY ACADEMY LIBERTAS PER CULTUM	Name of School	Barclay Academy
	AUP review Date	September 2022
	Date of next Review	September 2023
	Who reviewed this AUP?	Matthew Laban

Acceptable Use Policy (AUP): Staff agreement form

Covers use of digital technologies in school: i.e. email, Internet, intranet and network resources, learning platform, software, equipment and systems.

- I will only use the school's digital technology resources and systems for Professional purposes or for uses deemed 'reasonable' by the Principal and Governing Body.
- I will not reveal my password(s) to anyone unless directed to do so by senior leadership or the police.
- I will not allow unauthorised individuals to access email / Internet / intranet / network, or other school / Trust systems.
- I will ensure all documents, data etc., are saved, accessed and deleted in accordance with the school's network and data security and confidentiality protocols.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will only use the approved, secure email system(s) for any school business.
(Which is currently: London Grid for Learning).
- I will only use the approved school email, school MLE or other school approved communication systems with pupils or parents/carers, and only communicate with them on appropriate school business.
- I will not browse, download or send material that could be considered offensive to colleagues.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the appropriate line manager / school named contact.
- I will not download any software or resources from the Internet that can compromise the network, or are not adequately licensed.
- I will not connect a computer, laptop or other device (including USB flash drive), to the network / Internet that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the school's recommended anti-virus, firewall and other ICT 'defence' systems.
- I will not use personal digital cameras or camera phones for taking and transferring images of pupils or staff and will not store images at home without permission.
- All images of pupils should be captured using school owned cameras and all data should be kept in school and transferred electronically to school servers.

- Before taking a school owned digital image capture device off site, I will ensure that any images already held on that device are backed up in school and will delete any images that clearly identify children or staff by name.
- During off-site visits, I will ensure that any digital image capture device is held securely by a member of staff.
- I will ensure that any students or staff are made aware of any photographs being taken and are given the opportunity to view these images on demand.
- I will not take any photographs without all involved being aware that images are being captured and the purpose for which they are being captured.
- I will not use a mobile internet device (phone, tablet or laptop/netbook) to access data or websites deemed unsafe or compromised by school, during any contact time.
- I will use the school's Learning Platform in accordance with school / and London Grid for Learning advice.
- I will ensure that any private social networking sites / blogs etc that I create or actively contribute to are not confused with my professional role.
- Any references to my professional role, while accessing or using social networking or other publicly accessible sites will not include the name of the school, any colleagues or any pupils in entries, profile or comments.
- I agree and accept that any computer or laptop loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.
- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I will embed the school's online safety curriculum into my teaching.
- I will only use Trust systems in accordance with any corporate policies.
- I understand that all Internet usage / and network usage can be logged and this information could be made available to my manager on request.
- I understand that failure to comply with this agreement could lead to disciplinary action.

User Signature

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent online safety policies.

I agree to abide by all the points above.

I wish to have an email account; be connected to the Intranet & Internet; be able to use the school's ICT resources and systems.

Signature Date

Full Name (printed)

Job title

School

Authorised Signature (Principal or Vice Principal)

I approve this user to be set-up.

Signature Date

Full Name (printed)