Lord Lawson of
Beamish Academy

LORD LAWSON OF BEAMISH ACADEMY

ONLINE SAFETY POLICY

Originator: James Pedlingham

Revision: 001

Reviewed by governing body: December 2022

Date of next review: December 2025

1. Introduction

1.1 It is the duty of Lord Lawson of Beamish Academy to ensure that every student in its care is safe. These principles apply to the digital and online environment.

1.2 ICT and online communications provide significant opportunities for enhancing learning. With these opportunities there comes a risk to all users. Our students 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.

1.3 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 the academy 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.

1.4 This policy aims to provide clear guidance on how to minimise risks and how to deal with any infringements. It is linked to the following academy policies:

- Safeguarding and child protection policy
- Health and safety policy
- Behaviour management policy
- Anti-bullying policy
- Data protection
- Personal Development policy

1.5 All users, both on and off site, need to be aware of the range of risks associated with the use of online technologies. At Lord Lawson of Beamish

Academy, we understand the responsibility to educate and inform our students on online safety issues, teaching them 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.

2. Roles and Responsibilities

2.1 The Designated Safeguarding Lead (DSL) and ICT Manager have responsibility for this policy.

2.2 Lord Lawson of Beamish Academy believes that it is essential for parents/carers to be fully involved with promoting online safety both in and outside of school. Parents/carers will be consulted to discuss online safety to seek to promote a wide understanding of the benefits and risks related to internet usage.

3. Staff Awareness

3.1 All teaching staff receive regular information and training on online safety issues and are made aware of their individual responsibilities relating to the safeguarding of children within the context of online safety.

3.2 All staff working with children are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms.

3.3 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.

3.4 They should know what to do in the event of misuse of technology.

3.5 A record of any misuse must be completed by staff as soon as possible if any incident relating to online safety occurs and must be presented directly to the Designated Safeguarding Lead (DSL).

4. E-safety in the Curriculum and Classroom

4.1 ICT and online resources are used increasingly across the curriculum. It is essential for online safety guidance to be given to pupils on a regular and meaningful basis. Any opportunities to promote e-safety should be identified and regular monitoring and assessment of our students' understanding of keeping themselves safe.

4.2 Every time staff and students log onto the network, they are required to sign an electronic agreement to be allowed access to the network. They are confirming they will adhere to the academy's Acceptable Use Policy (statement) and it provides an opportunity to remind users to follow the academy's ICT guidelines.

4.3 The academy provides opportunities to teach about online safety within a range of curriculum areas and computing lessons. Educating students on the dangers of technologies that may be encountered outside school will also be carried out via Personal Development lessons.

The following topics are covered:

- advice on how to look after online safety
- recognising online sexual exploitation
- stalking and grooming
- relevant laws applicable to using the internet; such as data protection and intellectual property
- respecting other people's information and images
- impact of cyber-bullying and know how to seek

5. Use of School and Personal Devices

Staff

5.1 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.

5.2 All personal devices connected to the WIFI are subject to the school's filtering restrictions.

5.3 Staff should not give their personal mobile phone numbers or e-mail addresses to students, 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 academy's phones and e-mail using the school system.

Students

5.4 The academy provides a student wireless network which is made available to students who have a compatible wireless device to enhance their educational activities including learning, research and administration.

5.5 Use of this provision is governed by the Academy's Acceptable Use Policy (statement). By logging onto the network, the user is deemed to have agreed to abide by this policy.

6. Use of Internet and e-mail

Staff

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

6.2 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.

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

6.4 Staff must immediately report to ICT 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 the academy 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

6.5 Under no circumstances should students 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 academy ensures that staff have access to their work email address when offsite, for use as necessary on academy business.

Students

6.6 All students are issued with their own personal academy e-mail addresses for use on the 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. Students should be aware that email communications can be accessed.

6.7 There is strong anti-virus and firewall protection on the network. Spam emails and certain attachments will be blocked automatically by the email system. If this causes problems for school work/research purposes, students should contact the ICT Manager for assistance. The ICT Manager in consultation with the Designated Safeguarding Lead will decide on the appropriateness of such sites.

6.8 Students should immediately report to the ICT 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.

6.9 Students must report any accidental access to materials of a violent or sexual nature directly to the ICT Manager or another member of staff. Deliberate access to any inappropriate materials by a student will lead to the incident being recorded and will be dealt with under the Behaviour policy. Students should be aware that all internet usage via the academy's systems and its Wi-Fi network is monitored.

7. Password Security

7.1 Students and staff have individual network logins, email addresses and storage folders. Students and staff are regularly reminded of the need for password security.

Everyone should:

- use a strong password (containing a combination of characters, 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.

8. Safe use of digital and video images

8.1 The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and students 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.

8.2 When using digital images, staff should inform and educate students 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).

8.3 Staff and volunteers are allowed to take digital/video images to support educational purposes. Any 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 students are appropriately dressed and are not participating in activities that might bring the individuals or the academy into disrepute.

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

8.5 Written permission from parents/carers will be obtained before photographs of students/pupils are published.

8.6 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.

9. Concerns and Complaints

9.1 As with all issues of safety at the academy, if a member of staff, a student or a parent/carer has a complaint or concern relating to online safety, prompt action will be taken to deal with it. Complaints of this nature should be addressed to the ICT Manager in the first instance, who will undertake an immediate investigation and liaise with the senior leadership team and any members of staff or pupils involved.