Online Safety Policy

Lord Grey Academy

Approved by:	LGB	**Date:** February 2023
Last reviewed on:	June 2022	**Policy Owner:** Rob Page
Next review due by:	February 2024	

Contents

1. Aims 3

2. Legislation and guidance 3

3. Roles and responsibilities 3

4. Educating students about online safety 5

5. Educating parents about online safety 6

6. Cyber-bullying 6

7. Acceptable use of the internet in the Academy 7

8. Students using mobile devices in the Academy 7

9. Staff using work devices outside the Academy 8

10. Student use of loaned computer equipment 8

11. How the Academy will respond to issues of misuse 8

12. Training 8

13. Monitoring arrangements 9

14. Links with other policies 9

Appendix 1: KS3 and KS4 acceptable use agreement (students and parents/carers/guardians) 10

Appendix 2: acceptable use agreement (staff, governors, volunteers and visitors) 11

Appendix 3: online safety training needs – self audit for staff 12

Appendix 4: online safety incident report log 13

Changes log 14

1. Aims

Our Academy aims to:

- Have robust processes in place to ensure the online safety of students, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole Academy community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

2. Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and it's advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for principals and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the Department's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on students' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

This policy complies with our funding agreement and articles of association.

3. Roles and responsibilities

3.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the associate principal to account for its implementation.

The governing board will coordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the Academy's ICT systems and the internet (appendix 3)

3.2 The Associate Principal

The associate principal is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the Academy.

3.3 The designated safeguarding lead

Details of the Academy's DSL and deputy DSL are set out in our child protection and safeguarding policy as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in the Academy, in particular:

- Supporting the associate principal in ensuring that staff understand this policy and that it is being implemented consistently throughout the Academy
- Working with the associate principal, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged using CPOMS (see appendix 4) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyberbullying are logged and dealt with appropriately in line with the Academy behaviour policy
- Updating and delivering staff training on online safety (appendix 3 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in the Academy to the associate principal and/or governing board

This list is not intended to be exhaustive.

3.4 The ICT manager

The ICT manager is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep students safe from potentially harmful and inappropriate content and contact online while at the Academy, including terrorist and extremist material
- Ensuring that the Academy's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the Academy's ICT systems on a regular basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged using CPOMS (see appendix 4) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the Academy behaviour policy

This list is not intended to be exhaustive.

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the Academy's ICT systems and the internet (appendix 2), and ensuring that students follow the Academy's terms on acceptable use (appendix 1)
- Working with the DSL to ensure that any online safety incidents are logged using CPOMS (see appendix 4) and dealt with appropriately in line with this policy

- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the Academy behaviour policy

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

- Notify a member of staff or the associate principal of any concerns or queries regarding this policy
- Ensure their student has read, understood and agreed to the terms on acceptable use of the Academy's ICT systems and internet (appendix 1)

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? - UK Safer Internet Centre
- Hot topics - Childnet International
- Parent fact sheet - Childnet International
- Lord Grey Academy - Helpful Links

3.7 Visitors and members of the community

Visitors and members of the community who use the Academy's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 2).

4. Educating students about online safety

Online safety often becomes an issue we need to deal with following national trends and developments. For example from time to time we are made aware of new threats or crazes that appear online. The Academy will respond to these current issues and concerns at all times and will amend the order of curriculum delivery to allow matters of the moment to be addressed. However, in general we will follow the national curriculum standards as follows:

Students will be taught about online safety as part of the curriculum:

In Key Stage 3, students will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns

Students in Key Stage 4 will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

By the end of secondary school, they will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online

- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours

The safe use of social media and the internet will also be covered in other subjects where relevant.

The Academy will use assemblies to raise students' awareness of the dangers that can be encountered online and may also invite speakers to talk to students about this.

5. Educating parents about online safety

The Academy will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the associate principal and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the associate principal.

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the Academy behaviour policy.)

6.2 Preventing and addressing cyber-bullying

To help prevent cyberbullying, we will ensure that students understand what it is and what to do if they become aware of it happening to them or others. We will ensure that students know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The Academy will actively discuss cyber-bullying with students, in PSHE, Tutor Time and assemblies, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

All staff, governors and volunteers (where appropriate) receive training on cyberbullying, its impact and ways to support students, as part of safeguarding training (see section 12 for more detail).

The Academy also sends information on cyberbullying to parents so that they are aware of the signs, how to report it and how they can support students who may be affected.

In relation to a specific incident of cyberbullying, the Academy will follow the processes set out in the Academy behaviour policy. Where illegal, inappropriate or harmful material has been spread among students, the Academy will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

Academy staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on students' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the Academy rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of Academy discipline), and/or
- Report it to the police

Any searching of students will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

Any complaints about searching for or deleting inappropriate images or files on students' electronic devices will be dealt with through the Academy complaints procedure.

7. Acceptable use of the internet in the Academy

All students, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the Academy's ICT systems and the internet (appendices 1-2). Visitors will be expected to read and agree to the Academy's terms on acceptable use if relevant.

Use of the Academy's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by students, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1 and 2.

8. Students using mobile devices in Academy

We have a **No Mobile Phones** rule at Lord Grey Academy. We accept that parents may wish students to have a phone for the journey to and from the Academy but they are **NOT** permitted to use them in the Academy. They must be switched off and placed in their Academy bag. If phones are seen, they will be confiscated and placed in Student Services in the first instance.

Additional instances of confiscation will lead to parents having to collect the phone and to have a meeting with the Head of Year. There are a small number of students who may need to use a mobile phone to

monitor a health condition. In all cases this requirement will be documented in the medical care plan for the individual student.

DISCLAIMER
Students are not required to have a mobile phone in the Academy and we support parents who make the decision that this is not necessary by ensuring that students are able to use the Academy landlines to contact parents in an emergency. Parents should contact the Academy via the landline. Any student who brings a mobile phone into the Academy does so at their own risk and the Academy will not be held responsible for any loss or damage.

Disciplinary Procedures
Any person failing to follow the terms and conditions of this policy will face sanctions and/or disciplinary action. Sanctions have included detentions, meetings with parents, banning from the internet, loss of access to the Academy network, exclusion and loss of place in the 6th Form.

9. Staff using work devices outside the Academy

Staff members using a work device outside the Academy must not use the device in any way which would violate the Academy's terms of acceptable use, as set out in appendix 2.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside the Academy. Any USB devices containing data relating to the Academy must be encrypted.

If staff have any concerns over the security of their device, they must seek advice from the ICT manager.

Work devices must be used solely for work activities.

10. Student use of loaned computer equipment

On occasions Lord Grey Academy may have to loan IT equipment to students to enable the student to access online learning during periods of long absence from the Academy.

Arrangements would be made via the students Year team and the Vice Principal for Curriculum. A loan agreement form would be signed by the student's parents/carer/guardian and a representative of Lord Grey Academy.

The loan agreement will detail the equipment loaned, its value and the length of the loan. Any damages are payable by the Parent/Carer/Guardian when the equipment is returned to Lord Grey Academy.

Lord Grey Academy has the right to recall any loan equipment to check on its condition and service the equipment during long term periods or due to a concern of use.

11. How the Academy will respond to issues of misuse

Where a student misuses the Academy's ICT systems or internet, we will follow the procedures set out in our policies on Acceptable use of ICT for Students Policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the Academy's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The Academy will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

12. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

The DSL deputy DSL will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

13. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety using CPOMS. An incident report log can be found in appendix 4.

This policy will be reviewed every year by the associate principal. At every review, the policy will be shared with the governing board.

14. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure

Appendix 1: KS3 and KS4 acceptable use agreement (students and parents/carers/guardians)

ACCEPTABLE USE OF THE ACADEMY'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STUDENTS AND PARENTS/CARERS/GUARDIANS

Name of student:

I will read and follow the rules in the acceptable use agreement policy

When I use the Academy's ICT systems (like computers) and get onto the internet in the Academy I will:

- Always use the Academy's ICT systems and the internet responsibly and for educational purposes only
- Only use them when a teacher is present, or with a teacher's permission
- Keep my username and passwords safe and not share these with others
- Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer/guardian
- Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others
- Always log off or shut down a computer when I'm finished working on it

I will not:

- Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails or in anyway directly or indirectly bully any other student or adult
- Log in to the Academy's network using someone else's details
- Arrange to meet anyone offline without first consulting my parent/carer/guardian, or without adult supervision.
- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Install any unauthorised software, or connect unauthorised hardware or devices to the Academy's network
- Access, modify or share data I'm not authorised to access, modify or share

If I bring a personal mobile phone or other personal electronic device into the Academy:

- I will not use it when on the Academy site without a staff members permission

I agree that the Academy will monitor the websites I visit and that there will be consequences if I don't follow the rules. I understand that this extends to use on Academy devices at home and accessing the Academy remotely.

Signed (student):	**Date:**

Parent/carer's/guardian's agreement: I agree that my child can use the Academy's ICT systems and internet when appropriately supervised by a member of the Academy staff. I agree to the

conditions set out above for students using the Academy's ICT systems and internet, and for using personal electronic devices in the Academy, and will make sure my child understands these.

Signed (parent/carer/guardian):	**Date:**

Appendix 2: acceptable use agreement (staff, governors, volunteers and visitors)

ACCEPTABLE USE OF THE ACADEMY'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS,VOLUNTEERS AND VISITORS
Name of staff member/governor/volunteer/visitor:
When using the Academy's ICT systems and accessing the internet in the Academy, or outside the Academy on a work device (if applicable), I will not: ● Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) ● Use them in any way which could harm the Academy's reputation ● Access social networking sites or chat rooms ● Use any improper language when communicating online, including in emails or other messaging services ● Install any unauthorised software, or connect unauthorised hardware or devices to the Academy's network ● Share my password with others or log in to the Academy's network using someone else's details ● Take photographs of students without checking with teachers first ● Share confidential information about the Academy, its students or staff, or other members of the community ● Access, modify or share data I'm not authorised to access, modify or share ● Promote private businesses, unless that business is directly related to the Academy
I will only use the Academy's ICT systems and access the internet in the Academy, or outside the Academy on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. I agree that the Academy will monitor the websites I visit and my use of the Academy's ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside the Academy, and keep all data securely stored in accordance with this policy and the Academy's data protection policy. I will let the designated safeguarding lead (DSL) and ICT manager know if a student informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use the Academy's ICT systems and internet responsibly, and ensure that students in my care do so too.	
Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 3: online safety training needs – self audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	**Date:**
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in the Academy?	
Do you know what you must do if a student approaches you with a concern or issue?	
Are you familiar with the Academy's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the Academy's acceptable use agreement for students and parents/carers/guardians?	
Do you regularly change your password for accessing the Academy's ICT systems?	
Are you familiar with the Academy's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

Appendix 4: online safety incident report log

ONLINE SAFETY INCIDENT LOG				
Date	**Where the incident took place**	**Description of the incident**	**Action taken**	**Name and signature of staff member recording the incident**

Changes Log

Changes made	Changed by	Date changed
Section 8, changed reference from Head of House to Head of Year.	Rob Page	10th June 2022
Section 10 changed reference from Head of House to Head of Year	Rob Page	10th June 2022
Change references from Principal to Associate Principal throughout	Rob Page	10th June 2022
Changed wording of student to child in Parent/ carer's/ guardian's agreement in Appendix 1	Rob Page	10th June 2022
Reference made to logging concerns in CPOMS	Rob Page	16th January 2023