Girls' Learning Trust

IT POLICY

Contents

Appendices

REVIEW

Last reviewed: May 2018
To be reviewed: Every 3 years, or as the need arises.

Policies may be subject to review and revision at any time, notwithstanding that the next review date has not been reached. Review dates are for guidance only; all policies will remain in force until a review has taken place and been formally approved by the Trust.

1. Policy Statement

1.1 The Girls' Learning Trust (the "Trust") IT systems and equipment are intended to support and enable education, promote effective communication and working practices across the Trust community, and to support the Trust's Development Plan. This policy outlines the standards the Trust requires users of these systems to observe, the circumstances in which the Trust will monitor use of these systems and the action that will be taken in respect of breaches of these standards.

1.2 The aim of this policy is to assist the Trust in protecting staff and students from inappropriate use of technology and its consequences. The Trust also aims to ensure the security of information held on systems and to comply with its legal obligations in this and other regards.

1.3 All staff and students are expected to comply with this policy at all times to protect the Trust's IT systems and equipment from unauthorised access and harm. Breach of this policy may be dealt with under the Trust's Disciplinary Policy (for staff) or the school's behaviour policy (for students).

1.4 This policy does not form part of any employee's contract of employment and may be amended at any time.

1.5 This policy deals with the use of the Trust's IT systems and equipment through email, the internet, telephones, mobile phones, fax machines, copiers, scanners, closed circuit television (CCTV) systems, and any other devices used to gain access to the Trust systems.

2. Who is covered by the Policy?

2.1 This policy covers all individuals working, or having contact with the Trust and/or schools (such as volunteers (including trustees, governors and members), contractors and guests) at all levels within the Trust (collectively referred to as staff and students in this policy).

2.2 Third parties who have access to the Trust's IT systems and equipment are also required to comply with this policy.

3. Personnel Responsible for Implementation of the Policy

3.1 The Trust Board has delegated responsibility for the effective operation of this policy to the Trust's Executive Group who has, in turn, delegated day-to-day responsibility for its operation to the Trust's IT Team. Responsibility for monitoring and reviewing the operation of this policy and making any recommendations for change to minimise risks to the Trust's operations also lies with the Trust's IT Team

3.2 The Trust's IT Team will deal with requests for permission or assistance under any provisions of this policy, subject to their primary tasks of maintaining the core

systems, and may specify certain standards of equipment or procedures to ensure security and compatibility.

3.2 All staff and students (as per paragraph 2) are responsible for the implementation of this policy. Any misuse of the Trust's IT systems or equipment should be reported to, the Trust's IT Team, a member of the Trust's Executive Group or a member of the School's Leadership Team

4. Equipment, Security and Passwords

4.1 Staff and students are responsible for the security of the equipment allocated to or used by them, and must not allow it to be used by anyone other than in accordance with this policy.

4.2 Staff and students are responsible for the security of their computers. If leaving a terminal unattended, or when leaving their office or classroom, they must ensure that they lock their computer or log off to prevent unauthorised users accessing the system in their absence.

4.3 Desktop PCs/computers and cabling for telephones or computer equipment should not be moved or altered without first consulting the IT support team.

4.4 Passwords are unique to each user and should be changed regularly to ensure confidentiality. Staff and students who have been issued with a laptop computer or any other device must ensure that they are kept secure at all times, especially when travelling. Passwords must be used to secure access to data kept on such equipment to ensure that confidential data is protected in the event of loss or theft. Staff and students should also be aware that when using equipment away from the workplace, documents could be read by third parties, for example by passengers on public transport looking over one's shoulder.

4.5 To comply with Data Protection obligations, access must only be made via your own authorised account, passwords must be kept confidential and not shared with anyone. It is forbidden for anyone to allow another person to use a PC with their network credentials.

5. Systems and Data Security

5.1 Staff and students must not delete, destroy or modify existing systems, programs, information or data which could have the effect of harming the Trust's interests or exposing the Trust to risk.

5.2 Staff and students must not download or install software from external sources without authorisation from the Trust's IT Team. This includes software programs, instant messaging programs, screensavers and inappropriate pictures and video clips. Incoming files and data should always be virus-checked. If in doubt, staff and students should seek advice from the Trust's IT Team.

5.3 The Trust monitors all emails passing through the system for viruses and inappropriate material. Staff and students should exercise caution when opening emails from unknown external sources or where, for any reason, an email attachment appears suspicious (for example, if its name ends in .exe). The IT Support Team should be informed immediately if a suspected virus is received. The Trust reserves the right to block access to attachments to emails for the purpose of effective use of the system and for compliance with this policy. The Trust also reserves the right not to transmit any email message.

5.4 Staff and students should not attempt to gain access to restricted areas of the network, or to any password-protected information, unless specifically authorised by a member of the Trust's Executive Group or Trust's IT Team.

5.5 Staff and students using laptop computers or Wi-Fi enabled equipment or remote access must be vigilant about their use outside the Trust and take any precautions required by the Trust's IT Team from time to time against importing viruses or compromising the security of the Trust's systems. These systems contain information which is confidential to the Trust and its students and/or is subject to data protection legislation. Such information must be treated with extreme care and in accordance with the Trust's Data Protection and Freedom of Information Policy.

5.6 Any sensitive data copied from the Trust's systems and used on personal equipment must be password protected. In addition, if any personal equipment which may contain any Trust related data, is lost or stolen, it must be reported to the Trust's IT Team as a matter of urgency.

5.7 Any personal equipment being passed to a new owner or disposed of must have any Trust data removed from the device before ownership is relinquished.

6. Email and Content

6.1 Email is a vital educational tool, but an informal means of communication, and should be used with great care and discipline. Staff and students should always consider if email is the most appropriate means for a particular communication and correspondence sent by email should be written as professionally as a letter or fax. Messages should be directed only to relevant individuals.

6.2 Staff and students must not send abusive, obscene, discriminatory, racist, harassing, derogatory or defamatory emails. Anyone who feels they have been harassed or bullied, or are offended by any material received, and wishes to take action should refer to the Staff Anti Harassment and Bullying Policy.

6.3 Staff and students should take care with the content of email messages, as incorrect or improper statements can give rise to claims for discrimination, breach of confidentiality or breach of contract. Staff and students should assume that email messages may be read by others and not include anything which is of a personal/confidential nature or which would offend or embarrass any reader, or themselves, if it were required to be published in the public domain.

6.4 Email messages may be disclosed in legal proceedings in the same way as paper documents. Deletion from a user's inbox or archives does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.

6.5 In general, staff and students should not:

6.5.1 Share passwords with other users or request passwords personally assigned to other members of staff and students without permission of a member of the Trust's Executive Group, or the Trust's IT Team;

6.5.2 Send or forward private emails at work which they would not want a third party to read;

6.5.3 Agree to terms, enter into contractual commitments or make representations by email unless appropriate authority has been obtained. A name typed at the end of an email is a signature in the same way as a name written at the end of a letter;

6.5.4 Send messages from another worker's computer or under an assumed name unless specifically authorised.

7. Use of the Internet

7.1 Staff and students should not access any web page or any files downloaded from the internet which could, in any way, be illegal or regarded as offensive, in bad taste or immoral. While some content may be legal in the United Kingdom, it may be in sufficient bad taste to fall within this prohibition, particularly within the Trust environment.

8. Personal Use of Systems

8.1 The Trust permits incidental personal use of the internet and the Trust email and telephone systems subject to certain conditions set out below. Personal use must be neither abused nor overused and the Trust reserves the right to withdraw this permission at any time.

8.2 The following conditions must be met for personal usage to continue:

8.2.1 Use must be minimal and take place substantially out of normal working hours

8.2.2 Use must not interfere with Trust commitments;

8.2.3 Use must not commit the Trust to any extra costs;

8.2.4 Use must comply with all other Trust policies.

8.3 Staff and students should be aware that personal use of the Trust systems may be monitored (see paragraph 9) and, where breaches of this policy are found, action may be taken under disciplinary procedures for staff and students (see paragraph 10).

9. Monitoring

9.1 The Trust's systems enable it to monitor telephone, email, voicemail, internet and other communications. Use of the Trust's systems is monitored to the extent permitted or as required by law. CCTV systems monitor the exterior of school

buildings and reception areas (such as the front entrance to each school) 24 hours a day. The data from CCTV systems is recorded.

9.2 The Trust reserves the right to retrieve the contents of email messages or check searches which have been made on the internet for the following purposes:

9.2.1 To monitor whether the use of the email system or the internet is legitimate and in accordance with this policy;
9.2.2 To find lost messages or to retrieve email messages lost due to computer failure;
9.2.3 In exceptional circumstances, and where appropriate, to access and/or delete confidential emails, of a sensitive nature, which have been sent, posted or otherwise disseminated in error to or from an employee's email account;
9.2.4 To assist in the investigation of wrongful acts;
9.2.5 To comply with any legal and safeguarding obligation.

10. Inappropriate Use and Disciplinary Procedures

10.1 Misuse or excessive use or abuse of the Trust's IT systems and equipment or email system, or inappropriate use of the internet in breach of this policy or of the Acceptable Use Statement (Appendix A) will be dealt with under the Trust Disciplinary Policy for staff or the school's student Behaviour Policy. Misuse of the internet can, in certain circumstances, constitutes a criminal offence.

10.2 The Trust's disciplinary procedures may be invoked in cases of:

10.2.1 Misuse of the email system or inappropriate use of the internet

10.2.2 Creation or propagation of chain letters;

10.2.3 Intentionally creating, viewing, accessing, transmitting or downloading any of the following material (this list is not exhaustive):

- pornographic material (e.g. written material, pictures/photographs, audio material, films and video clips of a sexually explicit nature);
- offensive, obscene, or criminal material;
- material which is liable to cause embarrassment to the Trust;
- a false or defamatory statement about any person or organisation;
- material which is discriminatory, offensive or derogatory;
- confidential information about the Trust or any of the staff and students or students;
- accessing any material where such access is unauthorised;
- any other statement which is likely to create any liability (whether criminal or civil, and whether for the employee or the Trust);
- material in breach of copyright.

10.3 Where a member of staff and/or student inadvertently views material that would fall into a category listed in 10.2, that person has a duty to report this to either their line

manager, a member of the Trust's Executive Group, a member of the School's Leadership Team or Trust's IT team.

10.4 Where evidence of misuse is found the Trust may undertake a detailed investigation in accordance with the Trust's disciplinary procedures, which could include the examination and disclosure of monitoring records.

11. BYOD Policy

11.1 Where a school within the Trust allows students to Bring Your Own Device (BYOD), all aspects of this policy fully apply, with the addition of the BYOD Protocols (Appendix B).

12. Records Retention Policy

12.1 Electronic material and data held on Trust IT systems must comply with the Trust Records Retention Policy.

12.2 Other materials, including home folders, email accounts and other system access such as VLE and Office 365, will generally be removed from the Trust's systems immediately. However, in the case of students leaving the school, this is amended to 3 months after the start of the school term following the users' leaving date (to allow for university applications and similar correspondence). In all cases, information held on 3rd party systems used by the Trust is subject to contractual obligations with those third parties, which may mean the data is removed immediately.

13. Subject Access Requests (SAR)

13.1 When a SAR is received by the Trust's IT Team via the Trust' Data Protection Officer, the school's email system, network storage and web filter logs will be searched for any data relating to the individual in question, in line with the Trust's Data Protection and Freedom of Information Policy.

13.2 The individual's first name and surname (or preferred name as held on the School's Management Information System or the Staff Code), will constitute the criteria of the search.

13.3 In the case of emails, the default search will be carried out by searching the subject and body of all emails sent within the three months prior to the SAR, unless a date range is specifically requested in the SAR.

14. Third Party Portals & Websites

14.1 Any third party portals or websites to be commissioned, which will require staff or student personal data to be submitted/uploaded, will require a Data Processing Agreement with the third party (compliant with the Trust Data Protection & FOI Policy), and may be subject to a GDPR impact assessment. Advice should be sought from the Trust IT Team.

APPENDIX A

ACCEPTABLE USE STATEMENT (FOR STUDENTS AND STAFF)

The IT and computer systems are owned by the Trust and are made available to students to further their education and to staff to enhance their professional activities including teaching, research, administration and management. The Trust's Acceptable Use Statement has been drawn up to protect all parties - students, staff and the school.

By using the Trust IT network (and/or BYOD solution), staff and students agree to the Acceptable Use Statement.

- Access must only be made via the authorised account and password, which must not be made available to any other person;
- All internet use should be appropriate to staff professional activity or students' education;
- Activity that threatens the integrity of the Trust IT systems, or that attacks or corrupts other systems, is forbidden; e.g. introducing a virus;
- Sites and materials accessed must be appropriate to work in the Trust. Users will recognise materials that are inappropriate and should expect to have their access removed if they access these materials. Inappropriate materials should be reported to the Trust's IT Team;
- The Trust reserves the right to examine or delete any files that may be held on its computer system and to monitor and log user activities on the Internet;
- Users are responsible for email they send and for contacts made that may result in inappropriate email being received The same professional levels of language and content should be applied as for letters or other media, particularly as email is often forwarded;
- Posting anonymous messages and forwarding chain letters is forbidden;
- Copyright of materials and intellectual property rights must be respected;
- Use of the Internet for personal financial gain, gambling, political purposes or advertising is forbidden;
- The Trust will not be held responsible for payment of any items ordered through the Internet, unless authorised by the Trust Finance Department;
- Other users' files must not be accessed;
- Students in the Trust will not give their home address or phone number to any person, nor use the internet to arrange to meet anyone, unless their parent/carer or teacher has given them permission.
- The use of memory sticks or any other form of removable storage is permitted. However, the user is responsible for checking said media for viruses before use.
- Data will be held in accordance with the Trust's Records Retention Policy. However, home folders, email accounts and other system access such as VLE and Office 365, will be removed from the Trust's systems 3 months after the users' leaving date.

For further and more comprehensive details relating to the use of the Trust's IT systems and equipment, please see the Trust IT Policy.

APPENDIX B

'Bring Your Own Device' BYOD Network Protocols (where in use)

Where a BYOD policy is in use (school specific arrangements apply), the principles from the relevant school's Behaviour for Learning Policy (or similar), particularly the Anti-bullying Policy (or similar), apply to the use of the BYOD network.

Students should keep mobile devices and earphones out of sight (e.g. in their blazer pockets or bags) unless given permission in a teaching class, or they are in an area at a time when use of them is permitted.

Photography or filming is not allowed at any time without the express permission of a member of staff.

Devices must not be connected to any mobile data networks while on site (3G, 4G etc.), only filtered use of the BYOD network is authorised. All users of the BYOD network are required to have a valid and up-to-date antivirus program installed and running.

Phones should be kept on silent at all times.

Network Rules

- Whilst they are allowed to connect to the BYOD network, students are only allowed to use their devices when instructed to or in the designated areas.
- The students bring their devices into school on the understanding that it is at their own risk and they are responsible for their own device.
- The BYOD will be filtered so that certain websites and apps are inaccessible.
- Confiscation of devices and withdrawal of access to the BYOD network can be applied as a sanction for misuse.

Lesson Time

- In delivering the curriculum, there can be no expectation that students will have a device/smart phone. If IT is a necessity then an IT suite should be used or the school tablets or laptops booked.
- Mobile/portable devices are only to be used within lesson time if permitted by the teacher in charge of the lesson.
- Students are not allowed to use cameras to film footage, capture photos or record audio of staff or fellow pupils without the express permission of a member of staff.
- When devices are in use within lessons, students are allowed to use them for the task set by the teacher, and must seek permission for other use.

Break/Lunch Times (and before/after lesson hours)

- Devices are allowed to be used at break/lunch times and before/after lesson hours in classrooms, the Hall and at all times in the library, Sixth Form study area, the Sixth Form common room and outside. However it is still the case that no photography or filming is allowed without express permission of a member of staff.
- Students **ARE NOT** allowed to use their devices, or have headphones in, while walking through corridors of the school or whilst in the canteen. Elsewhere, audio from devices should be through headphones only.