Online Safety Policy

for all staff

Online Safety Policy

Contents

1 Introduction

1.1 The use of technology continues to be an important component of safeguarding young people. Technology, whilst providing many opportunities for learning also provides a platform that can facilitate harm. Keeping Children Safe in Education categorises online safety into three broad areas:

- **Content**: being exposed to illegal, inappropriate or harmful material; for example pornography, fake news, racist or radical and extremist views;
- **Contact**: being subjected to harmful online interaction with other users; for example commercial advertising as well as adults posing as children or young adults; and
- **Conduct**: personal online behaviour that increases the likelihood of, or causes, harm; for example making, sending and receiving explicit images, or online bullying.

1.2 It is with these three categories in mind that this policy outlines the roles, responsibilities and procedures for ensuring online safety.

2 Aims

2.1 This policy aims to set out the Trust's position in how it will strive to provide a safe environment for all of the school community whilst using ICT within the Trust, and how it will also strive to ensure that its members also use ICT, including their own personal devices, in a safe and responsible manner whilst outside of the Trust's grounds.

2.2 This policy will detail the individual responsibilities of each of the key people in the Trust who have a role to play in fulfilling this policy and its related procedures.

2.3 This policy applies to all staff, pupils, governors and parents of the Trust community. It should be read in conjunction with the supporting policies and related information that is detailed below.

2.4 The Constellation Trust believes that ICT can and should be used to enrich the education of all pupils. ICT also provides the staff of the Trust with a great many tools to help them play their part in providing the pupils of the school their education. Whilst the Trust sees the benefits of using this technology, it is also aware of the potential risks that the internet, ICT and related technology can pose. The Trust believe that online safety is the responsibility of the whole Trust community, and that all members of that community have their own part to play in ensuring that everyone can gain from the benefits that the internet and ICT afford to teaching and learning, whilst remaining safe.

2.5 Social Networking is becoming an increasingly popular tool within our environment to support learning, encourage creative and appropriate use of the internet and to publish and share content. These technologies need to be used in a safe and responsible way, and appropriate online behaviour encouraged. Although we encourage staff to use social networking to promote learning within the Trust, we also expect staff to maintain a professional level of conduct in their use of these types of technologies.

3 Risks & Responsibilities

3.1 Risks of ICT use and the Internet

The Trust has identified the following risks that ICT and the internet can pose to its community (this list is by no means exhaustive, but means to highlight some of the main areas of risk that the school has identified):

- Obsessive use of the internet and ICT
- Exposure to age-inappropriate materials
- Inappropriate or illegal behaviour
- Physical danger or sexual abuse
- Being subjected to harmful online interaction with other users
- Inappropriate or illegal behaviour by Trust staff
- Actions that bring the Trust into disrepute
- Online grooming or child exploitation

4 Creating a Safe ICT Learning Environment

4.1 The Trust believes that the best way to provide a safe ICT learning environment can be summarised as follows:

1. Create an infrastructure of whole-Trust awareness, designated responsibilities, policies and procedures. This is achieved by:
    - Raising awareness of the risks of ever-changing technology that is both emerging and already embedded in the Trust community.
    - Ensuring that the Online Safety policy and education programme adapts to meet these new and emerging technologies and is reviewed as incidents occur.
    - Establishing a clear understanding of the responsibilities of all of those involved with the education of children, with regards to Online Safety.
    - Ensuring that the Trust's policies and procedures are effective and kept up to date, and also make clear to all members of the Trust community what is acceptable when using ICT and the internet.

2. Make use of effective technological tools to ensure the safe use of the internet and Trust ICT systems. These include:
    - Firewall protection to the Trust's network.
    - Virus protection of all relevant IT equipment connected to the Trust's network.
    - Filtering, logging and content control of the school's internet connection.
    - Monitoring systems.

3. Develop an Online Safety education programme for the whole Trust. This will consist of:
    - An on-going education programme for the pupils in the Trust, so that they are given the tools to formulate and develop their own parameters of acceptable behaviour and take these with them when they leave the Trust.
    - Continued Professional Development for staff to ensure that they are equipped to support the pupils in the Trust, and are also fully aware of their responsibilities in using ICT, both in and out of the Trust.
    - An on-going education programme for parents, carers and the wider community so that they have the knowledge and tools available to support the actions of the Trust in these matters.
    - Explaining why harmful or abusive images on the Internet might be inappropriate or illegal.
    - Explaining why accessing age inappropriate, explicit, pornographic or otherwise unsuitable or illegal videos is harmful and potentially unsafe.
    - Explaining how accessing and / or sharing other people's personal information or photographs might be inappropriate or illegal.
    - Teaching why certain behaviour on the Internet can pose an unacceptable level of risk, including talking to strangers on social networking; how to spot an unsafe situation before it escalates, and how illegal practices such as grooming can develop.
    - Exploring in depth how cyber bullying occurs, how to avoid it, how to stop it, how to report it and how to deal with the consequences of it.

5 Headteacher's/CEO's Responsibilities

1. To take ultimate responsibility for online safety whilst delegating the day-to-day responsibility to the Chief Finance and Operating Officer (CFOO), Head of Digital Solutions and RM.
2. To ensure that the CFOO and the members of the online safety teams are given enough time, support and authority to carry out their remit.
3. To ensure that the LAB is kept informed of the issues and policies.
4. To ensure that the appropriate funding is available to support the technological infrastructure and CPD training for the online safety programme.

6 LAB's Responsibilities

1. To ensure the Designated Safeguarding Governor considers online safety as a part of the regular review of child protection and safeguarding.
2. To support the Headteacher and CFOO to ensure that the correct policies and procedures are in place, and that the funding required to achieve these policies and procedures is available.
3. To help in the promotion of online safety to parents.

7 CFOO's Responsibilities (through the Head of Digital Solutions and RM)

1. To develop and review the appropriate online safety policies and procedures.
2. To develop management protocols so that any incidents are responded to in a consistent and appropriate manner.
3. To work with the appropriate members of staff to develop a staff CPD programme to cover all areas of online safety inside and outside of the Trust environment.
4. To work with the appropriate members of staff to develop an online safety education programme for the pupils.
5. To work with the appropriate members of staff to develop a parental awareness programme for online safety at home.
6. To maintain a log of all online safety incidents that occur in the school.
7. To recommend reviews of technological solutions, procedures and policies based upon analysis of logs and emerging trends.
8. To meet with the Designated Safeguarding Leads regularly to discuss online safety and progress.
9. To liaise with any outside agencies as appropriate.
10. To maintain an appropriate level of professional conduct in their own internet use, both within and outside the Trust.

8 Designated Safeguarding Lead's Responsibilities

1. To seek professional development on the safety issues relating to the use of the internet and related technologies, and how these relate to young people.
2. To liaise with the CFOO on specific incidents of misuse.
3. Take a proactive role in the online safety education of the Trust's pupils.
4. Develop systems and procedures for supporting and referring pupils identified as victims or perpetrators of online safety incidents.
5. To maintain an appropriate level of professional conduct in their own internet use, both within and outside the Trust.

9 Managed Service Provider (RM) Responsibilities

1. To perform regular audits and checks of the Trust's networked systems to look for signs of misuse or inappropriate files. Any such findings would need to be reported to the CFOO, Headteacher and Police if necessary.
2. Review the technological systems upon any discovery or breach of the Acceptable Use Policy (AUP), to ensure that the same breach does not happen again.
3. Liaise with the pastoral team if any breach can be traced back to an individual pupil.
4. Liaise with the CFOO and Headteacher if any breach can be traced back to an individual member of staff.

5. Provide the technological infrastructure to support the online safety policies and procedures.
6. Report any network breaches of the Trust's Acceptable Use Policy or Online Safety Policy to the CFOO / Head of Digital Solutions.
7. To maintain an appropriate level of professional conduct in their own internet use, both within and outside the Trust.

10 Curriculum Director's / Subject Leaders' Responsibilities

1. To work with the CFOO to develop an area / departmental policy to ensure that online safety is embedded in their areas of teaching practice, where appropriate.
2. To maintain an appropriate level of professional conduct in their own internet use, both within and outside the Trust.
3. Any requests for social media posts at Sirius Academy West or Sirius Academy North to go through the Head of Digital Solutions.

11 Heads of Year / 6th Form Pastoral Officer's Responsibilities

1. To act as a key member of staff, and first point of contact for the Trust's online safety team.
2. To support the CFOO in the development and maintenance of appropriate policies and procedures relating to pupil welfare.
3. To develop and maintain their own knowledge of online safety issues.
4. To ensure that any incidents of ICT misuse are dealt with through the correct channels, in line with the ICT Acceptable Use Policy, Behaviour Policy and Online Safety Policy.
5. To ensure that any pupils who experience problems when using the internet are appropriately supported, working with the CFOO and DSL as required.
6. To maintain an appropriate level of professional conduct in their own internet use, both within and outside the Trust.

12 Special Educational Needs Coordinator's Responsibilities

1. To develop and maintain a knowledge of online safety issues, with regard as to how they may affect children and young people with additional educational needs.
2. To develop and maintain additional policies and online safety materials in conjunction with the CFOO, tailored to meet the needs of SEN pupils.
3. To liaise with parents and carers of SEN pupils to raise awareness of the Trust's online safety position and how the parents can support the Trust's position.
4. To maintain an appropriate level of professional conduct in their own internet use, both within and outside the Trust.

13 Classroom Teachers, Teaching Assistants, Resource Centre Staff (West) and Cover Supervisors' Responsibilities

1. To develop and maintain a knowledge of online safety issues, with regard to how they might affect children and young people.

2. To implement Trust and departmental online safety policies through effective classroom practice.

3. To ensure any incidents of ICT misuse are reported through the correct channels, following the Trust's Child Protection Procedure.

4. To ensure that the necessary support is provided to pupils who experience problems when using the internet, and that issues are correctly reported to the CFOO and the pastoral team.

5. To plan classroom use of ICT facilities so that online safety is not compromised.

6. To maintain an appropriate level of professional conduct in their own internet use, both within and outside the Trust.

4. Any requests for social media posts at Sirius Academy West or Sirius Academy North to go through the Head of Digital Solutions.

14 Pupil's Responsibilities

1. To uphold all Trust online safety and ICT policies.
2. To report any misuse of ICT within the Trust to a member of staff.
3. To seek help or advice from a teacher or trusted adult if they, or another pupil experience problems online.
4. To communicate with their parents or carers about online safety issues and to uphold any rules regarding online safety that may exist in the home.

15 Parents' and Carers' Responsibilities

1. To help and support the Trust in promoting online safety.
2. To discuss online safety concerns with children and to show an interest in how they use technology.
3. To take responsibility for learning about new technologies and the risks they could pose.
4. To model safe and responsible behaviour in their own use of the internet.
5. To discuss any concerns they may have about their children's use of the internet and technology with the Trust.

16 Procedures & Implementation

16.1 The Trust, through the CFOO, will ensure that all staff are aware of the policies and procedures being implemented to meet the Online Safety remit. There will be information available to all staff about the technologies that are already in use at the Trust as well as new and emerging technologies that they may come across in their professional practice. All staff will be given the opportunity to feedback into the Trust's online safety discussions, be given clear guidance to what the procedures are and know who they should speak to regarding any issues.

16.2 In the first instance, all staff will receive a basic introduction into the online safety programme in the Trust and be directed towards the resources that have been made available.

16.3 An area of each school's website contains relevant resources and links to information regarding the safe use of new technologies within the Trust environment.

16.4 The CFOO will work with the HR Team and Assistant Headteacher responsible for CPD to ensure that the school's induction and CPD programmes include adequate provision for the delivery of online safety training.

16.5 Online safety will form a part of the Child Protection Induction for new staff starters and direct them towards the existing policies, procedures, resources and courses of action.

17 Pupils

17.1 The pupils in the Trust will be made aware that there is a whole school approach to online safety and their roles and responsibilities within this e-Safe environment will be made clear to them. Pupil members will be invited to participate in the future planning and discussions regarding online safety and their opinions will be regularly gauged as to the effectiveness of the provision.

17.2 Through individual Year assemblies, pupils will be made aware of policies and methods of enforcing these policies.

17.3 Sixth Form students will be made aware of the Trust's position regarding online safety in their induction programme. A follow-up meeting will be held for all Year 13 pupils to make them aware and refresh their understanding.

18 Parents and Carers

18.1 The parents and carers of the Trust will be made aware of policies and procedures and how they can help in ensuring that the Trust schools are e-Safe schools. We will ensure that parents and carers can access information regarding the risks of new technologies, but also how they can ensure these technologies are being used safely.

18.2 An area on the school's website contains useful links and information for parents and carers regarding online safety. The website also contains the Trust's online safety policy, the ICT AUP and the Child Protection Policy.

18.3 Parents will also be updated on a regular basis regarding new apps and websites that pupils are accessing via the Wake Up Wednesday advice on our social media platforms and parental bulletins.

19 Firewall

19.1 The school has a perimeter firewall, which is supplied by Smoothwall with filtering policies managed by our Managed Service Provider RM, via a Trust Smoothwall management Server. This physical hardware device sits at the edge of the network and allows only specific traffic in and out of the network. All intrusion attempts from both sides of the network can be logged and analysed for security audits.

19.2 The responsibility lies with RM for ensuring that the firewall is correctly configured and that intrusion logs are regularly checked. Where changes to filtering policies are required, RM will contact the CFOO / Head of Digital Solutions to make sure changes are applied at Trust sites where required. Staff should only request changes to filtering policies via the DSL's and then the Head of Digital Solutions who will then instruct RM to amend if appropriate. The risk register held by The Trust will then be updated.

20 Anti-Virus Protection

20.1 The Trust, via RM has anti-virus protection which comprises a number of security tools to protect our network including; anti-virus, auto patching applications and malware redirect detection. The school also have an Enterprise License for Microsoft's Endpoint Protection. This anti-virus software is installed on Microsoft Windows based servers.

20.2 It is the responsibility of RM to ensure that all necessary computers on the Trust's network are running current anti-virus software and that regular scans are performed. RM receive daily updates on scans performed around site and will act upon any suspicious results from either computers or computer connected storage devices. If a virus out-break happens, RM must notify the CFOO / Head of Digital Solutions and as soon as possible isolate the infection.

20.3 Devices for staff should connect to the Domain network using their computer credentials to authenticate - this wireless network is ring-fenced by a firewall to protect internal network devices and only allow certain internal applications to connect. Visitors must obtain a login from RM and use the school visitor wireless network (guest Wi-Fi), which is the most strictly filtered connection (equivalent to student level) to provide guests an internet connection - secure sites are also not logged on this wireless network. No devices being brought into school should be connected to the school's ICT network, other than RM managed devices via Intune.

21 Filtering and Logging of Internet Access

21.1 The Trust has a web caching and proxy server that contains accredited filter lists. This enables the Trust (via RM) to log all Internet traffic in the Trust and allow different sites to different groups of users. This server ensures that all internet use on the Trust's network is logged to an individual user of the network, with the exception of guest devices connected to guest Wi-Fi as the users are 'unknown'. If an online safety incident requires it, all Internet access logs of any pupil or staff member can be retrieved to support any required processes.

21.2 It is the responsibility of the CFOO and RM to ensure that all computers connected to the Trust's network only receive an Internet connection by going through the proxy server. RM, on request of the CFOO or the Head of Digital Solutions, will add any sites that have been discovered through online safety incidents to the block lists of the filtering server.

22 Monitoring Systems

22. 1 The Trust has many different monitoring systems at its disposal;

- All files stored on the Trust's servers can be searched and checked
- Teachers can monitor the pupils use of computers within the IT Suites they are in through the RM Tutor software
- All computer use is monitored centrally against a set of predefined word lists and use or viewing of inappropriate text is logged with a screen grab and the details of the offence, user and time it occurred
- Any incident that has a sanction attached to it is entered into the school's MIS system
- Computer use is live monitored using Smoothwall Monitor Managed Service with incidents alerted to the CFOO / Head of Digital Solutions and RM.

22.2 RM can perform a scan of all staff and pupil home drives for all images and identify any inappropriate images saved. If any inappropriate images are found, RM will notify the CFOO / Head of Digital Solutions, providing the user name involved, full name of the user, date and time discovered, details of the incident or violation.

22.3 The monitoring system will monitor all users (staff and pupils) the same and the client will be installed on all Trust owned computers. The difference between staff and pupils, with regards to this monitoring system, will be the method in which those logs are reviewed.

22.4 RM and the CFOO / Head of Digital Solutions can access and review the logs of the silent monitoring system for the staff and respond accordingly to any breaches of the AUP or other online Safety incidents recorded.

22.5 Any incident that has a sanction attached will be entered into the MIS system using the behaviour type of ICT AUP Breach. These incidents can then be reported upon and shared with the relevant Pastoral Teams as required.

22.6 Where incidents raise concern regarding a child's welfare, they will be also recorded on our online Child Protection Monitoring System (CPOMS) where a pattern of concern can be identified if appropriate.

22.7 Currently, school-owned iPads do not have individual monitoring on them, as due to the nature of the device, you cannot identify the user at any given time. As such, they are filtered through the web proxy with the most restrictive student policy applied.

23 Online Safety Education

23. 1 All pupils in the Trust will receive an on-going online safety education programme.

23.2 This programme will inform the pupils of the issues and potential risks of using the internet and emerging technologies. It will also equip them with the knowledge to ensure they are adequately protected and informed when in these environments as new technology is adopted. They will be given the information required to know who they can talk to and what their rights are if they do experience issues whilst using the internet.

23.3 It has been developed in line with DfE guidance and covers:

- How to evaluate what pupils see online
- How to recognise techniques used for persuasion
- How to recognise acceptable and unacceptable online behaviour
- How to identify online risks
- How and when to seek support

23.4 Primary schools follow the Jigsaw PSHE programme and within this, the various staying safe aspects are incorporated.

23.5 Secondary schools' PSHE curriculum is under constant review to include emerging trends in pupils' online use and to address new uses as they arise. Currently this is covered in Years 7 to 11.

23.6 The Trust will follow the Safer Internet Day programme and deliver those resources through Year assemblies. Form tutors (Lesson 1) will be informed about the content being delivered, and asked to discuss the content after the assembly is given so that pupils have an opportunity to raise any concerns or issues from this information.

23.7 The Post-16 team will work with the CFOO / Head of Digital Solutions to ensure that there is an adequate online Safety education programme within the Post-16 Curriculum, and that the pastoral support team are up to date with the issues within their area. The online safety education programme will be delivered through the Post-16 PSHE programme.

23.8 The PSHE and Personal Development curriculum will be regularly reviewed to ensure that it has appropriate and relevant online safety content incorporated into its programme.

23.9 The SENCO will work with the CFOO / Head of Digital Solutions to ensure that there are accessible and adequate resources available for SEND pupils of the school to access the same online safety education as the rest of the Trust.

24 Responding to a concern

24.1 Appendix 1 outlines the process regarding concerns being raised relating to online safety. In the first instance any concern should be reported to the pupil's Head of Year/Pastoral Team in secondary schools and the DSL in primary schools.

24.2 As a Trust, we proactively work to ensure the safety of our pupils both in-school and online. We do not have the capacity to police all online activity outside of school, however where actions of a pupil online go against our code of conduct, as outlined in the School's Behaviour for Learning Policy, we may sanction pupils, following the expectations set out in our Behaviour for Learning Policy.

24.3 Where actions taken by pupils online pose a risk to them or others, they will be dealt with in line with our Child Protection Procedure, conducting appropriate risk assessments and ensuring minimal disruption to any victim, where appropriate.

25 School Social Media Accounts

25.1 The Trust controls social media accounts for Sirius Academy North and Sirius Academy West. Each primary school has various staff that manage their accounts.

25.2 Whilst all social media is different, and constantly evolving there are some key expectations for colleagues using social media in school, which are as follows:

- Any colleague wishing to set up a school or departmental social media account should first seek approval from the Trust and give reasons behind the decision.
- All social media must be set up to ensure that that there can be no private communication or Direct Messaging between the account and the accounts of pupils.
- A log of all social media accounts in schools should be kept by the Trust.
- Passwords should not be shared between colleagues and one colleague should take overall responsibility for the account and its content.
- Users should follow the expectations and responsibilities of colleagues outlined above.

25.3 As stated above, social media is constantly changing and as such advice should be sought from the Trust where appropriate.

25.4 The Trust no longer uses the Twitter/X social media platform.

25.5 It is strongly recommended that comments are not enabled for all posts.

26 Supporting Policies and Related Information

26.1 Constellation Trust supporting policies:

- ICT AUP
- Child Protection Policy & Procedure
- Code of Conduct for Staff
- Pupil Behaviour for Learning Policy

27 Procedure for Policy Implementation

27.1 The procedural document for this policy is attached as an appendix.

- Appendix 1 – Online Safety Incident Reporting Flowchart

Appendix 1 - Responding to incidents of misuse (Flow Chart)