Online Safety Policy

Aims and Scope of the Policy

This policy applies to all members of the Stockport Academy community (including staff, students/students, volunteers, parent/carer/carers/carers, visitors, community users) who have access to and are users of Stockport Academy digital technology systems, both in and out of the organisation.

The Education and Inspections Act 2006 empowers Headteachers/Principals to such extent as is reasonable, to regulate the behaviour of students/students when they are off the Stockport Academy site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online-bullying or other online safety incidents covered by this policy, which may take place outside of the Academy but is linked to membership of the Academy. The Education Act 2011 increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

Stockport Academy will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parent/carers/carers of incidents of inappropriate online safety behaviour that take place out of school.

Stockport 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 school community in its use of technology; and
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

Legislation and guidance

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

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

It also refers to the DfE'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 considers the National Curriculum computing programmes of study. This policy also complies with our funding agreement and articles of association.

Roles and responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the school/academy.

4.1 The Local Governing Body (LGB)

The LGB has overall responsibility for monitoring this policy and holding the Principal to account for its implementation.

The LGB will co-ordinate 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 school's ICT systems and the internet; and
- Support the monitoring and development of e-safety policy and awareness through the Governors Pastoral Committee and nominated safeguarding governor.

The safeguarding governor who oversees online safety alongside the Governors Pastoral subcommittee is responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy.

This will be carried out by the LGB receiving regular information about online safety incidents and monitoring reports. A member of the LGB has taken on the role of Online Safety/Safeguarding Governor and this role includes:

- regular meetings with the Online Safety Co-ordinator/Deputy Designated Safeguarding Lead;
- attendance at Pastoral sub-committee meetings;
- regular monitoring of online safety incident logs;
- regular monitoring of filtering/change control logs; and
- reporting to relevant LGB meeting .

4.2 The Principal and Senior Leadership Team

The Principal is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

The Principal has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day-to-day responsibility for online safety will be delegated to the Online Safety Lead.

The Principal and the Designated Safeguarding Lead/ Vice Principal should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff and should refer to the Academy Safeguarding policy, United Learning Whistleblowing policy, Local Authority Designated Officer and United Learning Safeguarding lead.

The Principal and Senior Leaders are responsible for ensuring that the Online Safety Lead/Safeguarding lead and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.

The Principal and Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

The Senior Leadership Team will receive regular monitoring reports from the Online Safety/ Safeguarding Lead – online safety incidents are also provided to the LGB termly as part of the Academy Safeguarding report.

Other responsibilities include:

- Coordinating participation in local and national events to promote positive online behaviour, eg Safer Internet Day;
- Ensuring that online safety is integrated with other appropriate school policies and procedures;
- Ensuring that online safety is promoted to parent/carers and carers and the wider community through a variety of channels and approaches;
- Working with the school/setting lead for data protection and data security to ensure that practice is in line with legislation.; and
- Reviewing and updating online safety policies, Acceptable Use Policies (AUPs) and other procedures on a regular basis (at least annually) with stakeholder input.

4.3 The designated safeguarding lead

Details of the school's Designated Safeguarding Lead (DSL) and Deputy Designated Safeguarding Lead (DDSL) are available on the Academy website.

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

- Supporting the Principal in ensuring that staff understand this policy and that it is being implemented consistently throughout the school;
- Working with the Principal, ICT manager and other staff, as necessary, to address any online safety issues or incidents;
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy;
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy;
- Through CPOMS, maintaining an online safety incident/action log to record incidents and actions taken as part of the school's safeguarding recording structures and mechanisms;
- Monitoring the school/settings online safety incidents to identify gaps/trends and update the education response to reflect need and to report to the school leadership team, Governing Body and other agencies as appropriate;
- Updating and delivering staff training on online safety;
- Liaising with other agencies including the Local Authority and the Trust and/or external services if necessary;

- Providing regular reports on online safety in school to the Principal and/or governing board;
- Acting as a named point of contact on all online safety issues and liaising with other members of staff and agencies as appropriate;
- Keeping up-to-date with current research, legislation and trends regarding online safety; and
- Meeting regularly with the governor responsible for on-line safety/Safeguarding.

4.4 The ICT network manager

The ICT network manager is responsible for:

- Putting in place appropriate filtering, safe security 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 school, including terrorist and extremist material;
- Providing a safe and secure technical infrastructure which supports safe online practices while ensuring that learning opportunities are still maximised;
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly. Ensuring that the school's ICT infrastructure/system is secure and not open to misuse or malicious attack;
- To ensure that suitable access controls and encryption is implemented to protect personal and sensitive information held on school-owned devices. Ensuring that appropriate anti-virus software and system updates are installed and maintained on all setting machines and portable devices;
- Conducting a full security check and monitoring the school's ICT systems on a weekly/fortnightly/monthly basis;
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files;
- Ensuring that the school's filtering policy is applied and updated on a regular basis and that responsibility for its implementation is shared with the online safety lead and DSL. Ensuring that the use of the setting's network is regularly monitored in order that any deliberate or accidental misuse can be reported to the online safety lead and DSL;
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy;
- Ensure that appropriately strong passwords are applied and enforced for all but the youngest users;
- Report any breaches or concerns to the Designated Safeguarding Lead, United Learning Technology Team and Leadership Team and together ensure that they are recorded on the e Safety Incident Log, and appropriate action is taken as advised; and
- Keeping up to date with relevant legislation as it relates to the security and safety of the technical infrastructure.

4.5 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 school's ICT systems and the internet and ensuring that students follow the school's terms on acceptable use;
- Working with the DSL/DDSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy;
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy;
- Identifying individuals of concern, and taking appropriate action by working with the designated safeguarding lead. Knowing when and how to escalate online safety issues, internally and externally;
- Reading and signing the school Acceptable Use Policies (AUPs) and adhering to them;
- Taking responsibility for the security of school/setting systems and data;
- Having an awareness of online safety issues, and how they relate to the children in their care;
- Modelling good practice in using new and emerging technologies and demonstrating an emphasis on positive learning opportunities;
- Embedding online safety education in curriculum delivery wherever possible;
- Being able to signpost to appropriate support available for online safety issues, internally and externally;
- Maintaining a professional level of conduct in their personal use of technology, both on and off site; and
- Taking personal responsibility for professional development in this area.

4.6 Parent/carers/Carers

Parent/carers/Carers are expected to:

- Notify a member of staff or the Principal of any concerns or queries regarding this policy;
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet;
- Read the school Acceptable Use Policy and encourage their children to adhere to them, adhering to them themselves where appropriate;
- Discuss online safety issues with their children, supporting the school in their online safety approaches, and reinforce appropriate safe online behaviours at home;
- Role model safe and appropriate uses of new and emerging technology;
- Identify changes in behaviour that could indicate that their child is at risk of harm online;
- Seek help and support from the school, or other appropriate agencies, if they or their child encounters online problems or concerns;
- Contribute to the development of the school/setting online safety policies;

- Use school systems, such as learning platforms, and other network resources, safely and appropriately; and
- Take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.

Parent/carers 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/carer factsheet - Childnet International
- Healthy relationships – Disrespect Nobody

4.7 Visitors and members of the community

Visitors and members of the community who access Stockport Academy systems or programmes, or use the school's ICT systems or internet as part of the wider academy provision will be made aware of this policy (when relevant) and will be expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use and sign a Community User Acceptable Use Agreement before being provided with access to academy systems.

4.8 Students

Students should:

- use Stockport Academy digital technology systems in accordance with the student/student acceptable use agreement;
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so;
- know and understand policies on the use of mobile devices and digital and on the taking/use of images and on online-bullying;
- understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the Academy's online safety policy covers their actions out of school, if related to their membership of the school;
- contribute to the development of online safety policies;
- read the Academy's Acceptable Use Policy (AUP) and adhere to it;
- respect the feelings and rights of others both on and offline;
- seek help from a trusted adult if things go wrong, and support others who may be experiencing online safety issues;
- take responsibility for keeping themselves and others safe online;
- take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies; and
- assess the personal risks of using any particular technology, and behave safely and responsibly to limit those risks.

Education/Training

5.1 Educating Students

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in online safety/digital literacy is therefore an essential part of Stockport Academy's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum is provided as part of Computing/PHSE/Assemblies and where appropriate in other lessons and is regularly revisited; and
- Key online safety messages are reinforced as part of a planned programme of assemblies and tutorial/pastoral activities.

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; and
- 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; and
- how to report a range of concerns.

By the end of secondary school, students 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; and

- 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.

Stockport Academy is aware that some children may be considered to be more vulnerable online due to a range of factors and will ensure that differentiated and ability appropriate online safety (e-Safety) education is given, with input from specialist staff as appropriate.

5.2 Educating Parent/carers/Carers

Many parent/carers and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's online behaviours. Parent/carers may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

Stockport Academy will therefore seek to provide information and awareness of internet safety to parent/carers and carers through:

- Curriculum activities;
- Letters, newsletters, web site;
- Parent/carers/carers evenings/sessions;
- High profile events/campaigns e.g. Safer Internet Day; and
- Reference to the relevant web sites/publications

This policy will also be shared with parent/carers.

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

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

5.3 Educating and training Staff/Volunteers

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy.

A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced.

All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the academy online safety policy and acceptable use agreements.

It is expected that some staff may identify online safety as a training need within the performance management process.

The DDSL will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.

The Online Safety Lead/DDSL will provide advice/guidance/training to individuals as required.

This online safety policy and its updates will be presented to and discussed by staff in staff/team meetings/training sessions.

5.4 Educating and training Governors

Online safety training is available to Members of the LGB which is of particular importance for those who are members of any group involved in technology/online safety/health and safety /safeguarding.

This may be offered in several ways:

- Attendance at training provided by the Local Authority/United Learning/National Governors Association/or other relevant organisation;
- Participation in Stockport Academy training/information sessions for staff or parent/carers this may include attendance at assemblies/lessons;
- Presentations made to the Pastoral governors sub committee;
- The online safety (e-Safety) policy will be provided to and discussed with members of staff as part of induction and will be reinforced and highlighted as part of school safeguarding practice.;
- To protect all staff and students, the school will implement Acceptable Use Policies which highlights appropriate online conduct and communication;
- Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential;
- Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff on a regular basis;
- Members of staff with a responsibility for managing filtering systems or monitoring ICT use will be supervised by the leadership team and will have clear procedures for reporting issues or concerns; and
- All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

Protecting children from online abuse

Reference NSPCC "Protecting children from online abuse"(16.3.22)

Online abuse is any type of abuse that happens on the internet, facilitated through technology like computers, tablets, mobile phones and other internet-enabled devices (Department for Education, 2018; Department of Health, 2017; Scottish Government, 2021; Welsh Assembly Government, 2018).

It can happen anywhere online that allows digital communication, such as:

- social networks
- text messages and messaging apps
- email and private messaging
- online chats
- comments on live streaming sites
- voice chat in games.

Children and young people can be revictimised (experience further abuse) when abusive content is recorded, uploaded or shared by others online. This could happen if the original abuse happened online or offline.

Children and young people may experience several types of abuse online:

- bullying/cyberbullying
- emotional abuse (this includes emotional blackmail, for example pressuring children and young people to comply with sexual requests via technology)
- sexting (pressure or coercion to create sexual images)
- sexual abuse
- sexual exploitation.

Children and young people can also be groomed online: perpetrators may use online platforms to build a trusting relationship with the child in order to abuse them. This abuse may happen online or the perpetrator may arrange to meet the child in person with the intention of abusing them.

6.1 Cyber-bullying

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 school behaviour policy.)

6.2 Emotional Abuse

Emotional abuse is the ongoing emotional maltreatment of a child, which can have a severe and persistent negative effect on the child's emotional development (Department for Education, 2020; Department of Health, 2017; Scottish Government, 2021; Wales Safeguarding Procedures Project Board, 2020). It's also known as psychological abuse.

Exposing a child to aggression, cruelty or abuse between other is also a form of emotional abuse (Doyle and Timms, 2014).

Most forms of abuse include an emotional element, but emotional abuse can also happen on its own.

Children can be emotionally abused by anyone:

- parent/carers or carers
- family members
- other adults
- other children

Online examples of emotional abuse can include (but are not limited to):

- verbal humiliation
- name-calling
- criticism
- restricting social interaction
- exploiting or corrupting
- encouraging a child to take part in criminal activities
- forcing a child to take part in activities that are not appropriate for their stage of development
- terrorising
- threatening violence
- bullying
- deliberately frightening a child
- deliberately putting a child in a dangerous situation

6.3 Consensual and non-consensual sharing of nudes and semi-nude images and or videos (Sexting)

Sexting is when people share a sexual message and/or a naked or semi-naked image, video or text message with another person. It's also known as nude image sharing.

Children and young people may consent to sending a nude image of themselves. They can also be forced or coerced into sharing images by their peers or adults online.

If a child or young person originally shares the image consensually, they have no control over how other people might use it.

If the image is shared around peer groups, it may lead to bullying and isolation. Perpetrators of abuse may circulate a nude image more widely and use this to blackmail a child and/or groom them for further sexual abuse.

It's a criminal offence to create or share explicit images of a child (anyone under the age of 18), even if the person doing it is a child. If reported to the police, they will make a record but may decide not to take any formal action against a young person.

6.4 Sexual Abuse

Child sexual abuse (CSA) is when a child is forced or persuaded to take part in sexual activities. This may involve physical contact or non-contact activities and can happen online or offline (Department for Education, 2018; Department of Health, Social Services and Public Safety, 2017; Scottish Government, 2021; Wales Safeguarding Procedures Project Board, 2020). Children and young people may not always understand that they are being sexually abused.

Contact abuse involves activities where an abuser makes physical contact with a child. It includes:

- sexual touching of any part of the body, whether the child is wearing clothes or not
- forcing or encouraging a child to take part in sexual activity
- making a child take their clothes off or touch someone else's genitals
- rape or penetration by putting an object or body part inside a child's mouth, vagina or anus.

Non-contact abuse involves activities where there is no physical contact. It includes:

- flashing at a child
- encouraging or forcing a child to watch or hear sexual acts
- not taking proper measures to prevent a child being exposed to sexual activities by others
- making a child masturbate while others watch
- persuading a child to make, view or distribute child abuse images (such as performing sexual acts over the internet, sexting or showing pornography to a child)
- making, viewing or distributing child abuse images
- allowing someone else to make, view or distribute child abuse images
- meeting a child following grooming with the intent of abusing them (even if abuse did not take place)
- sexually exploiting a child for money, power or status (child sexual exploitation).

6.5 Child Sexual Exploitation

Child sexual exploitation (CSE) is a type of child sexual abuse. It occurs where an individual or group takes advantage of an imbalance of power to coerce, manipulate or deceive a child or young person under the age of 18 into sexual activity (Department for Education, 2017; NIdirect, 2021; Scottish Government, 2018; Wales Safeguarding Procedures Project Board, 2020).

Children and young people in sexually exploitative situations and relationships are persuaded or forced to perform sexual activities or have sexual activities performed on them in return for gifts, drugs, money or affection.

CSE can take place in person, online, or using a combination of both.

Perpetrators of CSE use a power imbalance to exploit children and young people. This may arise from a range of factors including:

- age
- gender
- sexual identity
- cognitive ability
- physical strength
- status
- access to economic or other resources (Department of Education, 2017).

Sexual exploitation is a hidden crime. Young people have often been groomed into trusting their abuser and may not understand that they're being abused. They may depend on their abuser and be too scared to tell anyone what's happening because they don't want to get them in trouble or risk losing them. They may be tricked into believing they're in a loving, consensual relationship.

Some children and young people are trafficked into or within the UK for sexual exploitation.

When sexual exploitation happens online, young people may be persuaded or forced to:

- have sexual conversations by text or online
- send or post sexually explicit images of themselves
- take part in sexual activities via a webcam or smartphone (Hamilton-Giachritsis et al, 2017).

Abusers may threaten to send images, video or copies of conversations to the young person's friends and family unless they take part in further sexual activity. Images or videos may continue to be shared long after the sexual abuse has stopped.

6.6 Radicalisation

Information taken from: https://www.getsafeonline.org/social-networking/online-radicalisation/

Radicalisation by extremist groups or individuals can be perpetrated via several means: face-to-face by peers, in organised groups in the community and, increasingly, online. Their targets are individuals or groups of people who can be easily led towards terrorist ideologies because of their experiences, state of mind or sometimes their upbringing.

However extremists attempt to influence vulnerable people, the internet invariably plays some kind of role … being widely used both to create initial interest, and as reinforcement to other means of communication. As is the case with everything it is used for, the internet enables considerably larger numbers of people to be reached, in a wider geographic area, and with less effort by the perpetrators.

The power of social media is well-known, and it is this that is the main channel for such grooming – be it Facebook, Twitter or the multitude of other sites and apps. Other online channels include chatrooms, forums, instant messages and texts. All are also used by extremists for their day-to-day communication, as is the dark web.

Social media is also used for research by extremists, making it easy for them to identify those who may be vulnerable from what they reveal in their profiles, posts/tweets, photos and friend lists.

6.7 The school's response to online abuse

To help prevent online abuse 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 school will actively discuss examples of online abuse with students, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover examples of online abuse. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

Staff, governors and volunteers (where appropriate) receive training on examples of online abuse its impact and ways to support students, as part of safeguarding training.

The school also sends information/leaflets on examples of online abuse to parent/carers so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of online abuse, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among students, the school 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.

Mobile Technologies

UL Policy: https://hub.unitedlearning.org.uk/sites/policies/Technology Policies/Bring Your Own Device Policy (Temporary School Closures).docx

Accessing United Learning Data using your own device policy: https://hub.unitedlearning.org.uk/sites/policies/Technology Policies/Accessing United Learning Data Using your Own Device Policy.docx

For more information, please refer to the Academy's Bring Your Own Device Policy.

1. Use of digital and video images

In line with the school's Image Use Policy, written permission from parent/carers or carers will always be obtained before images/videos of students are electronically published. The Academy seeks permission from stakeholders regarding the use of images from all parent/carers/carers annually – policy is shared with parent/carers via student online/planners.

Any images, videos or music posted online will comply with the intellectual property rights and copyright

Link to United Learning Copyright Policy: https://hub.unitedlearning.org.uk/sites/policies/Technology Policies/Copyright & PRS - images, videos, music, notation, software.docx

2. Data Protection

When sharing information staff will ensure they comply with group data protection policies and keep records of disclosures as required by these policies.

3. Technical – infrastructure/equipment, filtering and monitoring

United Learning/Stockport Academy will be responsible for ensuring that the Academy infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

- Stockport Academy technical systems will be managed in ways that ensure that the Academy meets recommended technical requirements outlined in Local Authority/UL guidance);
- There will be regular reviews and audits of the safety and security of academy technical systems;
- Servers, wireless systems and cabling will be securely located and physical access restricted;
- All users will have clearly defined access rights to academy technical systems and devices;

- All users will be provided with a username and secure password by the Academy ICT network manager who will keep an up-to-date record of users and their usernames. Users are responsible for the security of their username and password.;
- The "master/administrator" passwords for the academy systems, used by the Network Manager will also available to the cluster network ICT manager and kept in a secure place;
- The network manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations;
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes;
- Internet filtering/monitoring is in place to ensure that children are safe from terrorist and extremist material when accessing the internet;
- Stockport Academy has provided enhanced/differentiated user-level filtering (allowing different filtering levels for different ages/stages and different groups of users – staff/students/students);
- Academy technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the acceptable use agreement;
- Any actual/potential technical incident/security breach should be reported to the ICT Network manager, the Principal, DSL, Vice Principal or the Data lead for the Academy.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, mobile devices, etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual devices are protected by up-to-date virus software;
- An agreed protocol is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school systems; and
- The use of removable media (e.g. memory sticks/CDs/DVDs) by users on school devices is not permitted.

4. Managing Email

Students may only use Academy provided email accounts for educational purposes.

All members of staff are provided with a specific Academy email address to use for any official communication.

Staff are permitted to contact students via their own school email account and students' school email accounts.

Staff must demonstrate safe and responsible online behaviour at all times.

Communication must take place within explicit professional boundaries and should only be in relation to the students' education.

Staff should ensure that communication is open and transparent/carer.

If communication by a student is deemed to be personal or inappropriate, staff should not respond and the line manager or safeguarding team should be alerted immediately.

The use of personal email addresses by staff for any official school/setting business is not permitted.

The forwarding of any chain messages/emails etc. is not permitted. Spam or junk mail will be blocked and reported to the email provider.

Any electronic communication which contains any content which could be subject to data protection legislation must only be sent using secure and encrypted methods.

Members of the school community must immediately tell a designated member of staff if they receive offensive communication and this should be recorded in the school online safety/ Safeguarding incident log.

Sensitive or personal information will only be shared via email in accordance with data protection legislation.

Caution should be taken on opening emails with attachments or clicking on links within; being conscious of the risks from malware.

Whole-class or group email addresses may be used for communication.

Access in school to external personal email accounts may be blocked.

School email addresses and other official contact details will not be used for setting up personal social media accounts.

Excessive social email use can interfere with learning and will be restricted.

5. How the school will respond to issues of misuse

It is hoped that all members of Stockport Academy will be responsible users of digital technologies, who understand and follow Academy policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported;
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure;
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).;
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below); and

- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:

    - Internal response or discipline procedures
    - Involvement by Local Authority/Academy Group or national/local organisation (as relevant).
    - Police involvement and/or action.

If content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:

- incidents of 'grooming' behaviour;
- the sending of obscene materials to a child;
- adult material which potentially breaches the Obscene Publications Act;
- criminally racist material;
- promotion of terrorism or extremism;
- offences under the Computer Misuse Act; or
- other criminal conduct, activity or materials.

Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all the above steps are taken as they will provide an evidence trail for the Academy and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

Specific student/staff misuse

Where a student misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour and ICT and internet acceptable use. 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 school'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 disciplinary procedures/staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

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

6. References, further reading and useful links

GOV.UK (30.6.2020), 'Guidance: Education for a Connected World', available at: https://www.gov.uk/government/publications/education-for-a-connected-world

LGfL (2021), 'Online Safety and Safeguarding', available at:

https://www.lgfl.net/online-safety/default.aspx

National Online Safety (2021), 'Online Safety Education for the Whole School Community', available at:

https://nationalonlinesafety.com/

NSPCC Learning 16.3.2022), 'Protecting children from online abuse', available at: https://learning.nspcc.org.uk/child-abuse-and-neglect/online-abuse

SWGfL (2020), '{school/academy} Online Safety Policy Template', available at: https://swgfl.org.uk/assets/documents/online-safety-policy-templates-without-appendicies.pdf

The Key (23.12.2020), 'Online safety policy: models and examples', available at: https://schoolleaders.thekeysupport.com/policy-expert/pastoral/online-safety-policy-model-examples/#section-0

United Learning (2021), 'Policies Portal', available at: https://hub.unitedlearning.org.uk/sites/policies

Action Fraud: www.actionfraud.police.uk
BBC WebWise: www.bbc.co.uk/webwise
CEOP (Child Exploitation and Online Protection Centre): www.ceop.police.uk
ChildLine: www.childline.org.uk
Childnet: www.childnet.com
Get Safe Online: www.getsafeonline.org
Internet Matters: www.internetmatters.org
Internet Watch Foundation (IWF): www.iwf.org.uk
Know the Net: www.knowthenet.org.uk
Lucy Faithfull Foundation: www.lucyfaithfull.org
Net Aware: www.net-aware.org.uk
Parent/carer Port: www.parent/carerport.org.uk
Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline
The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
Think U Know: www.thinkuknow.co.uk
UK Safer Internet Centre: www.saferinternet.org.uk
Virtual Global Taskforce: www.virtualglobaltaskforce.com