Online Safety Policy

Summer Term 2017

Review Date: Summer Term 2018

Introduction

This Online Safety policy recognises the commitment of our partnership to keeping staff and pupils safe online and acknowledges its part in the partnership's overall safeguarding policies and procedures. It shows our commitment to meeting the requirement to keep pupils safe when using technology. We believe the whole school community and partnership can benefit from the opportunities provided by the internet and other technologies used in everyday life. The Online Safety Policy supports this by identifying the risks and the steps we are taking to avoid them. It shows our commitment to developing a set of safe and responsible behaviours that will enable us to reduce the risks whilst continuing to benefit from the opportunities. We wish to ensure that all members of the partnership are aware that unlawful or unsafe behaviour is unacceptable and that, where necessary disciplinary or legal action will be taken. We aim to minimise the risk of misplaced or malicious allegations being made against adults who work with pupils.

Our expectations for responsible and appropriate conduct are set out in our Acceptable Use Policies (AUP) which we expect all traineesto follow.

As part of our commitment to Online Safety we also recognise our obligation to implement a range of security measures to protect the network and facilities from attack, compromise and inappropriate use and to protect partnership data and other information assets from loss or inappropriate use.

Acknowledgements

This policy is based on an original document 'YHGfL Guidance for Creating an E-Safety Policy' written by Yorkshire and Humberside Grid for Learning. It has been adapted by Kirklees Learning Service for use in Kirklees Schools.

The scope of policy

- This policy applies to the whole partnership including the Director; strategic partners; all staff employed directly or indirectly by the partnership, visitors and all trainees
- The partnership will ensure that any relevant or new legislation that may impact upon the provision for online safety within school will be reflected within this policy
- The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school 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 related incidents covered by this policy, which may take place out of school, but is linked to membership of the school
- The Education Act 2011 gives the school the power to confiscate and search the contents of any mobile device if the Headteacher believes it contains any material that could be used to bully or harass others
- The school will clearly detail its management of incidents within this policy, associated behaviour and anti-bullying policies and will, where known, inform parents and carers of incidents of inappropriate online behaviour that take place out of school

Implementation of the policy

- The partnership will ensure all trainees are aware of the contents of the school Online Safety Policy and the use of any new technology within school
- All trainees of our ICT equipment will sign the relevant Acceptable Use Policies
- Online safety will be taught as part of the core training
- The Online Safety Policy will be made available to trainees by the website

Responsibilities of the School Community within the partnership schools

We believe that online safety is the responsibility of the partnership and that everyone has their part to play in ensuring all members of the community are able to benefit from the opportunities that technology provides for learning and teaching. The following responsibilities demonstrate how each member of the community will contribute.

Please read the individual school's E-safety policy and note each stakeholder's responsibilities.

Responsibilities of all Trainees

- Read, understand and help promote the SCITT's and the host school's online safety policies and guidance.
- Read, understand and adhere to the staff AUP
- Take responsibility for ensuring the safety of sensitive SCITT and school data and information
- Develop and maintain an awareness of current online safety issues, legislation and guidance relevant to their work
- Maintain a professional level of conduct in their personal use of technology at all times
- Ensure that all digital communication with pupils is on a professional level and only through school based systems, NEVER through personal email, text, mobile phone social network or other online medium
- Embed online safety messages in learning activities where appropriate
- Supervise pupils carefully when engaged in learning activities involving technology
- Ensure that pupils are told what to do should they encounter any material or receive a communication which makes them feel uncomfortable
- Report all online safety incidents which occur in the appropriate log and/or to their line manager
- Respect, and share with pupils the feelings, rights, values and intellectual property of others in their use of technology in school and at home

The following local and national guidance are acknowledged and included as part of our Online Safety Policy:

1. Kirklees LSCB Guidance

The Kirklees Safeguarding Children's Board Procedures and Guidance

Kirklees Safeguarding procedures will be followed where an online safety issue occurs which gives rise to any concerns related to child protection. In particular we acknowledge the specific guidance in:

Section 1.4.6 Child Abuse and Information Communication Technology

This section of the Kirklees Safeguarding procedures covers awareness of, and response to, issues related to child abuse and the internet. In particular, we note and will follow the advice given in the following section:

Section 7 Actions to be taken where an Employee has Concerns about a Colleague

This provides guidance on the action to be taken if an employee has either information or reason to suspect that a colleague is accessing indecent images of children.

2. Government Guidance

Cyberbullying: Advice for Headteachers and School Staff (DfE 2014)

Advice on Child Internet Safety 1.0 Universal Guidelines for Providers (DfE and UKSIC 2012)

3. Kirklees Guidance

The following Kirklees Guidance documents are included as part of this Online Safety Policy:

Kirklees First Responders Guidance for School Staff

Use of the Internet

We provide the internet to

- Support training
- Support the professional work of trainees as an essential professional tool
- Enhance the SCITT's management information and business administration systems
- Enable electronic communication and the exchange of data and information between staff and trainees

Users are made aware that they must take responsibility for their use of, and their behaviour whilst using the SCITT and school IT systems or a school/SCITT provided laptop or device and that such activity can be monitored and checked.

All users of the SCITT/school IT or electronic equipment will abide by the relevant Acceptable Use Policy (AUP) at all times, whether working in a supervised activity or working independently.

Learning and Teaching

We believe that the key to developing safe and responsible behaviours online for everyone within our SCITT and school community lies in effective education. We know that the internet and other technologies are embedded in our trainees' lives, not just in school but outside as well, and we believe we have a duty to help prepare our trainees to benefit safely from the opportunities that these present.

We will deliver a planned core training session on online safety knowledge and understanding and to ensure that trainees have a growing understanding of how to manage the risks involved in online activity.

Trainees will be reminded that third party content should always be appropriately attributed so as not to breach copyright laws.

We will discuss, remind or raise relevant online safety messages with trainees routinely wherever suitable opportunities arise. This includes the need to protect personal information and to consider the consequences their actions may have on others.

Emails

Email is regarded as an essential means of communication and the SCITT and school supplies all members of the SCITT community with an e-mail account for SCITT and school based communication. Communication by email betweentrainees, pupils and parents will only be made using the school email account and should be professional and related to school matters only.

- As part of the curriculum pupils are taught about safe and appropriate use of email
- It is the personal responsibility of the email account holder to keep their account secure
- School will set clear guidelines about when pupil-staff communication via email is acceptable
- Under no circumstances will staff contact pupils, parents or conduct any school business using a personal email addresses
- Responsible use of personal web mail accounts on SCITT and school systems is permitted outside teaching hours

Publishing Online Content

The partnership maintains editorial responsibility for any partnership initiated website or publishing online to ensure that the content is accurate and the quality of presentation is maintained. The partnership maintains the integrity of the SCITT web site by ensuring that responsibility for uploading material is always moderated and that passwords are protected.

We ask all trainees to sign an agreement about taking and publishing photographs and videos (in publications and on websites) and this list is checked whenever an activity is to be published.

Publishing Online Content Outside School

Trainees are encouraged to adopt similar safe and responsible behaviours in their personal use of blogs, wikis, social networking sites and other online publishing outside school as they are in school.

Material published by pupils, governors and staff in a social context which is considered to bring the school into disrepute or considered harmful to, or harassment of another pupil or member of the school community will be considered a breach of school discipline and treated accordingly.

Using images and videos

We recognise that many aspects of the training can be enhanced by the use of multi-media and that there are now a wide and growing range of devices on which this can be accomplished.

For their own protection trainees should never use a personal device (mobile phone, digital camera or digital video recorder) to take photographs of pupils.

Using Mobile Phones

Unauthorised or secret use of a mobile phone or other electronic device, to record voice, pictures or video is forbidden. Publishing of such material on a web site which causes distress to the person(s) concerned will be considered a breach of school discipline, whether intentional or unintentional. The person responsible for the material will be expected to remove this immediately upon request. If the victim is another pupil or staff member we do not consider it a defence that the activity took place outside school hours.

Managing and Securing IT Systems

The partnership will ensure all access to the SCITT's IT system is as safe and secure as reasonably possible. Servers and other key hardware and infrastructure are located securely with only appropriate staff permitted access.

- A firewall is maintained and virus and malware protection is installed on all appropriate hardware and is kept active and up to date
- All administrator passwords for the SCITT's IT systems are kept secure and available to at least two members of staff
- The wireless network is protected by a secure logon which prevents unauthorised access. New users can only be given access by the ICT Technician
- We ensure that a secure and robust username and password convention exists for all system access
- We provide trainees with a unique individually named username account
- Trainees are given guidance in creating secure passwords and a complex password policy is enforced for all staff members
- We do not allow anyone except technical staff to download and install software onto the network
- Trainees are aware of their obligation to keep sensitive data secure when working on computers outside school
- All devices taken off site, e.g. laptops, tablets, removable media or phones, are secured to protect sensitive and personal data and not left in cars or insecure locations
- We have full back up and recovery procedures in place for trainee data
- Details of all school-owned hardware and software are recorded in an inventory
- Disposal of any ICT equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007

Internet Filtering

Web filtering of Internet content is provided by YHGFL. This ensures that all reasonable precautions are taken to prevent access to illegal, unsuitable and/or inappropriate content. However, it is not possible to guarantee that all access to this material will never occur and we believe it is important to build resilience in trainees in monitoring their own internet activity.

Trainees are informed about the actions to take if inappropriate material is discovered and this is supported by notices around school. However deliberate access of inappropriate or illegal material will be treated as a serious breach of the AUP and appropriate sanctions taken.

Trainees are encouraged to check out websites they wish to use prior to lessons for suitability of content.

Online Safety Incidents

All online safety incidents are recorded in the SCITT Online Safety Log which is regularly reviewed.

Any incidents where trainees do not follow the Acceptable Use Policy will be dealt with following the MAT's normal behaviour or disciplinary procedures.

In situations where a trainee is made aware of a serious online safety incident concerning pupils or staff, they will inform the Online Safety Lead or the Headteacher who will then respond in the most appropriate manner. If the incident involves another trainee the trainee will inform the Director of the SCITT.

Instances of online bullying will be taken very seriously by the partnership and dealt with using the partnership's anti-bullying procedures. The SCITT recognises that trainees as well as pupils may be victims and will take appropriate action in either situation, including instigating restorative practices to support the victim.

Incidents which create a risk to the security of the SCITT network, or create an information security risk, will be referred to the partnership's Online Safety Lead and ICT Technician and appropriate advice sought and action taken to minimise the risk and prevent further instances occurring, including reviewing any policies, procedures or guidance. If the action breaches partnership policy, then appropriate sanctions will be applied.

The SCITT reserves the right to monitor equipment on their premises and to search any technology equipment, including personal equipment with permission, when a breach of this policy is suspected.

Dealing with a Child Protection issue arising from the use of technology:

If an incident occurs which raises concerns about child protection or the discovery of indecent images on the computer, then the procedures outlined in the Kirklees Safeguarding Procedures and Guidance will be followed.

Section 1.4.6 Child Abuse and Information Communication Technology

The following activities constitute behaviour which we would always consider unacceptable (and possible illegal):

- Accessing inappropriate or illegal content deliberately
- Deliberately accessing downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- Continuing to send or post material regarded as harassment or of a bullying nature after being warned
- Trainees using digital communications to communicate with pupils in an inappropriate manner (for instance, using personal email accounts, personal mobile phones, or inappropriate communication via social networking sites)

The following activities are likely to result in disciplinary action:

- Any online activity by a member of the SCITT which is likely to adversely impact on the reputation of the SCITT
- Accessing inappropriate or illegal content accidentally and failing to report this
- Inappropriate use of personal technologies (e.g. mobile phones) at training, school or in lessons Sharing files which are not legitimately obtained e.g. music files from a file sharing site
- Using SCITT/school or personal equipment to send a message, or create content, that is offensive or bullying in nature or could bring the SCITT into disrepute

- Attempting to circumvent SCITT filtering, monitoring or other security systems
- Circulation of commercial, advertising or 'chain' emails or messages
- Revealing the personal information (including digital images, videos and text) of others by electronic means (e.g. sending of messages, creating online content) without permission
- Using online content in such a way as to infringe copyright or which fails to acknowledge ownership (including plagiarizing of online content)
- Transferring sensitive data insecurely or infringing the conditions of the Data Protection Act 1998

The following activities would normally be unacceptable; in some circumstances they may be allowed e.g. as part of training or by a system administrator to problem solve

- Accessing social networking sites, chat sites, instant messaging accounts, email or using a mobile phone for personal use during lesson time
- Accessing non-educational websites (e.g. gaming or shopping websites) during lesson time
- Sharing a username and password with others or allowing another person to log in using your account
- Accessing SCITT ICT systems with someone else's username and password
- Deliberately opening, altering, deleting or otherwise accessing files or data belonging to someone else

Acceptable Use of Policy for Trainees

- Any content I post online (including outside school time) or send in a message will be professional and responsible and maintain the reputation of the SCITT

- To protect my own privacy, I will use a school email address and school telephone numbers (including school mobile phone) as contact details for pupils and their parents

- If I use any form of electronic communication for contacting pupils or parents I will use the school's system, never a personal account

- I will only use my personal mobile phone during non-teaching time; it will be kept on silent mode during lessons and training sessions except in an emergency situation with the agreement of the Headteacher or Session Facilitator

- I will never use my personal mobile phone or other personal electronic equipment to photograph or video pupils, trainees or members of the SCITT team

- Taking and publishing of photographs and videos will only be done with the permission of pupils and/or their parents for agreed school activities. This also includes the permission of other trainees and SCITT staff

- I will take all reasonable steps to ensure the safety and security of school and SCITT IT equipment which I take off site and will remove anything of a personal nature before it is returned to school and the SCITT

- I will take all reasonable steps to ensure that all personal laptops and memory devices are fully virus protected and that protection is kept up to date

- I will report any accidental access to material which might be considered unacceptable immediately to the Headteacher and/or Director and ensure it is recorded.

- Confidential school/SCITT information, pupil information or data which I use will be stored on a device which is encrypted.

- Computers will be locked or fully logged off before being left unattended

- I understand that I have the same obligation to protect school/SCITT data when working on a computer outside school

- I will report immediately any accidental loss of confidential information so that appropriate action can be taken

- I understand that the school/SCITT may monitor or check my use of IT equipment and electronic communications

- I understand that by not following these rules I may be subject to the school's and SCITT's disciplinary procedures

Visitors to the School Acceptable Use Policy for Community Users of School/SCITT Computers

As a user of the school's and SCITT's computers I recognised that it is my responsibility to follow school/SCITT procedures for the safe use of computers and that I have a responsibility to ask for advice if I am not sure of a procedure.

- I confirm that I will use all means of electronic communication equipment belonging to the school/SCITT and any personal devices which I bring into school/SCITT in a responsible manner and in accordance with the following guidelines:
- I will only use the school/SCITT computers for purposes related to the work I am completing in the school.
- I will not use a personal device I have brought into school/SCITT for any activity which might be considered inappropriate in a school/SCITT centre.
- I will not use my personal mobile phone or other electronic equipment to photograph or video pupils, trainees or SCITT staff
- I will not publish photographs or videos of pupils, trainees or SCITT staff without the knowledge and agreement of the school, the pupils, the trainees and/or SCITT staff.
- I will not give any personal contact details such as email address, mobile phone number or social media details to any pupil in the school. I will not arrange to video conference or use a web camera with pupils unless specific permission is given by the school.
- I will take all reasonable steps to ensure the safety and security of school/SCITT IT equipment, including ensuring that any personal devices or memory devices are fully virus protected and that protection is kept up to date.
- I will report any accidental access to material which might be considered unacceptable immediately to a senior member of staff and ensure it is recorded.
- I will not publish or share any information I have obtained whilst working in the school/SCITT on any personal website, blog, social networking site or through any other means, unless I have permission from the school.

- I understand that the school/SCITT has the right to examine or delete any files that may be held on its computer system, to monitor any websites visited and emails exchanged and, if necessary to report anything which may constitute a criminal offence.
- I understand that by not following these rules my use of school/SCITT facilities may be withdrawn.