skipton girls' high school
an engineering academy

Skipton Girls' High School

The Safe Use of Technology Policy

Introduction

This policy applies to all members of Skipton Girls' High School (including staff, students, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of the school.

The Education and Inspections Act 2006 empowers Head teachers to such extent as is reasonable, to regulate the behaviour of students when they are off the school site and empowers members of staff to impose sanctions for inappropriate behaviour. This is pertinent to incidents of bullying, or other on-line incidents covered by this policy, which may take place outside of the school but is linked to membership of the school. The 2011 Education Act 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.

E-Safety risks to children include cyber-bullying, the invasion of privacy, accessing inappropriate materials such as pornography, and communicating with strangers.

Skipton Girls' High School will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e - safety behaviour that take place out of school.

We recognise that all children and young people are at risk of online sexual exploitation. We will ensure that SGHS' E-safety procedures are robust and that children and young people are taught online safety skills so they know:

- Online risks
- How to recognise unsafe online contact
- To be confident to report concerns about themselves or others to in school staff

Roles and Responsibilities

Governors are responsible for the approval of 'The Use of Safe Technology Policy' and for reviewing the effectiveness of the policy. A member of the Local Governing Body has taken on the role of Child Protection and Safeguarding. This will include:

- meetings with the E - Safety Co -ordinator
- monitoring of e - safety incident logs
- monitoring of filtering / change control logs
- reporting to relevant Governors / Board / committee / meeting

The **Headteacher – Mrs Jenn Plews** has a duty of care for ensuring the safety (including e - safety) of members of the school community, though the day to day responsibility for E-safety has been delegated to the E-Safety Co -ordinator – **Mrs Fiona McMillan (Assistant Headteacher)**.

- The Headteacher and the Senior Leadership Team are responsible for procedures to be followed in the event of a serious e - safety allegation being made against a member of staff.
- The Headteacher and Senior Leaders are responsible for ensuring that the e -safety and other relevant staff receive suitable training to enable them to carry out their e - safety roles and to train other colleagues, as relevant.
- The Headteacher and Senior Leaders are responsible for managing a system to allow for monitoring and support of those in school who carry out the internal e - 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 receive regular monitoring updates during SLT meetings under Safeguarding from the E - Safety Co -ordinator.

The role of the e -Safety Coordinator is to:

- Lead the e - safety committee.
- Take day to day responsibility for e- safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents.
- Ensure that all staff are aware of the procedures that need to be followed in the event of an e - safety incident taking place.
- Provide training and advice for staff.
- Liaise with school technical staff.
- Receive reports of e - safety incidents and creates a log of incidents to inform future e - safety developments.
- Meet regularly with Safeguarding Governor to discuss current issues, review incident logs and filtering /change control logs.
- Attend relevant meeting / education committee of Local Governing Body.
- Report regularly to Senior Leadership Team.

The Network Manager is responsible for ensuring:

- That the school's technical infrastructure is secure and is not open to misuse or malicious attack.
- That the school meets required e - safety technical requirements.
- That users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.
- The filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.
- that they keep up to date with e - safety technical training in order to effectively carry out their e -safety role and to inform and update others as relevant.
- That the use of the network / internet / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher /Senior Leader: E- Safety Coordinator for investigation / action / sanction.
- That monitoring software / systems are implemented and updated as agreed in school policies.

Teaching and Support Staff are responsible for ensuring that:

- They have an up to date awareness of e -safety matters and of the current school e - safety policy and practices.
- They have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP).
- They report any suspected misuse or problem to the Headteacher / Senior Leader, e-Safety Coordinator / Officer.

- All digital communications with students / parents / carers are on a professional level and only carried out using official school systems.
- E - safety issues are embedded in all aspects of the curriculum and other activities.
- Students understand and follow the e - safety and acceptable use policies.
- Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- They monitor the use of digital technologies, mobile devices, cameras etc.
- In lessons and other school activities (where allowed) and implement current policies with regard to these devices.

The **Child Protection / Safeguarding Designated Person – Mrs Fiona McMillan** is trained in e - safety issues and is aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on - line contact with adults / strangers
- potential or actual incidents of grooming
- cyber - bullying

Students:

- Are responsible for using the school digital technology systems in accordance with the Student / Pupil Acceptable Use Policy.
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber - bullying.
- Should understand the importance of adopting good e - safety practice when using digital technologies out of school and realise that the school's E- Safety Policy covers their actions out of school, if related to their membership of the school.

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school/ will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website / VLE and information about national / local e - safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website / VLE and on - line student records
- their children's personal devices in the school

Policy Statements

Education – 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 e-safety is therefore an essential part of the school's e – safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

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

- A planned e-safety curriculum should be provided as part of ICT/ Computing / PHSE / other lessons and should be regularly revisited.
- Key e- safety messages should be reinforced as part of a planned programme of gatherings and tutorial activities.
- Students should be taught in all lessons to be critically aware of the materials / content they access on - line and be guided to validate the accuracy of information.
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Students / pupils should be helped to understand the need for the student / pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.
- Staff should act as good role models in their use of digital technologies the internet and mobile devices.
- Where students are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff can temporarily remove those sites from the filtered list for the period of study.

Education – parents / carers

Many parents and carers have only a limited understanding of e-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 on-line behaviours. Parents 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. The school will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, web site, VLE
- Parents / Carers evenings / sessions
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications

Education & Training – Staff / Volunteers

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

Training will be offered as follows:

- A planned programme of formal e - safety training will be made available to staff. This will be regularly updated and reinforced.
- An audit of the e-safety training needs of all staff will be carried out regularly.
- It is expected that some staff will identify e - safety as a training need within the performance management process.
- All new staff should receive e - safety training as part of their induction programme, ensuring that they fully understand the school e - safety policy and Acceptable Use Agreements. This E - Safety policy and its updates will be presented to and discussed by staff in staff meetings / INSET days.
- The E -Safety Coordinator will provide advice / guidance / training to individuals as required.

Training – Governors

Governors take part in e - safety training / awareness sessions with particular importance for those who are members of any sub-committee / group involved in technology / e - safety / health and safety / child protection.

This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association / or other relevant organisation.
- Participation in school training / information sessions for staff or parents (this may include attendance at assemblies / lessons).

Technical – infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school 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 need to ensure that the relevant people named in the above sections will be effective in carrying out their e - safety responsibilities:

- School technical systems will be managed in ways that ensure that the school academy meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of school technical systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to school technical systems and devices.
- All users will be provided with a username and secure password by Mr Paul Clifton who will keep an up to date record of users and their usernames.
- The "master / administrator" passwords for the school ICT system, used by the Network Manager must also be available to the Headteacher or other nominated senior leader and kept in a secure place (e.g. school safe).
- Mr Paul Clifton- ICT 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.
- The school has provided enhanced / differentiated user - level filtering.
- School technical staff regularly monitors and records the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. The school infrastructure and individual workstations are protected by up to date virus software.
- An agreed policy is in place regarding the extent of personal use that users (staff / students / pupils / community users) and their family members are allowed on school devices that may be used out of school.
- An agreed policy is in place that allows staff to / forbids staff from downloading executable files and installing programmes on school devices.
- An agreed policy is in place regarding the use of removable media (e.g. memory sticks / CDs / DVDs) by users on school devices.

- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Sixth Form

The school has a set of clear expectations and responsibilities for all users - covered by our AUP (acceptable use policy).
The school adheres to the Data Protection Act principles 'We do'.

- All users are provided with and accept the Acceptable Use Agreement - AUP.
- All network systems are secure and access for users is differentiated - different levels of filtering for 6th compared to lower school i.e. access to external email and YouTube.
- Where possible these devices will be covered by the school's normal filtering systems, while being used on the premises - our filtering covers all staff and students.
- All users will use their username and password and keep this safe - yes.
- Students receive training and guidance on the use of personal devices - this is covered by way of e-safety gatherings etc.
- Any device loss, theft, change of ownership of the device will be reported as in the BYOD policy - not applicable, students own devices are their responsibility.
- Any user leaving the school will follow the process outlined within the BYOD policy - as above.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Kept no longer than is necessary.
- Processed in accordance with the data subject's rights.
- Secure.
- Only transferred to others with adequate protection.

The school must ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".
- It has a Data Protection Policy.
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA).
- Risk assessments are carried out.
- It has clear and understood arrangements for the security, storage and transfer of personal data.
- Data subjects have rights of access and there are clear procedures for this to be obtained.
- There are clear and understood policies and routines for the deletion and disposal of data.
- There is a policy for reporting, logging, managing and recovering from information risk incidents.
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties.

- There are clear policies about the use of cloud storage / cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner's Office.

Social Media - Protecting Professional Identity

All schools, academies and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools/academies and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school liable to the injured party. Reasonable steps to prevent predictable harm must be in place.
The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions.
- Risk assessment, including legal risk.

School staff should ensure that:

- No reference should be made in social media to students / pupils, parents / carers or school staff.
- They do not engage in online discussion on personal matters relating to members of the school community.
- Personal opinions should not be attributed to the school /academy or local authority.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

This policy will be reviewed and updated on a regular basis in line with government legislation and at least on a yearly basis.

Reviewed: November 2015 Author: FAM/ JNP
Next Reviewed: November 2016