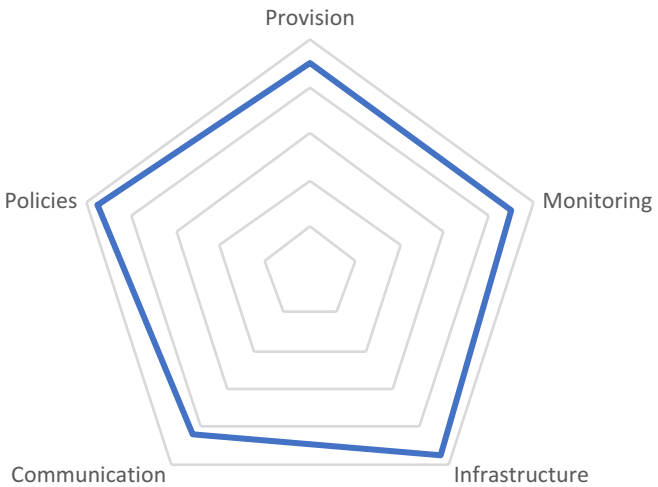
NATIONAL ONLINE SAFETY REVIEW

TRINITY ACADEMY

Date: 2/2/2018



NOTE: All areas covered within the report are scored from 1(lowest) to 5(highest)

OVERVIEW

The school has a good level of online safety and is very aware of the importance of online safety for learners, parents and staff. Staff have a good understanding of their online safety responsibilities inside of and outside of school.

KEY AREAS FOR IMPROVEMENT

- Implement automatic notifications from filtering provisions to the Designated Safeguarding Lead to ensure that all potential risks are identified quickly and acted upon with suitable process.
- Working towards GDPR develop a data retention policy, considering how long data should be held for after an ICT user exit from your school.

OVERALL SCORE: 4

1. Online Safety Provision

Online safety Provision

This phase reviews the present provision in place for all stakeholders. Evidence could include Schemes of Work, Use of external agencies, examples of intervention, staff training records, governor training records, evidence of stakeholder training.

LEARNERS

Due to the vulnerable nature of students tailored interventions take place with individuals when and as required, this is aided in its implementation due to the small size of the school.

Online safety is given a prominent focus within the curriculum and the subject is visited as part of internet safety week and other relevant focus days.

Online Safety education is reactive and additional sessions are used to cover new apps and current school issues.

STAFF

Staff training is delivered via safeguarding training, there is no discrete Online Safety training in place. More focused specific online safety training should be implemented to safeguard all stakeholders.

COMMUNITY

Due to the large catchment of the school parental training is difficult. Support material is provided at timely intervals (e.g. parental controls guidance at Christmas time) and material is referenced via the school website.

Suggested Actions for Improvement:

Identify students that are more at risk to online safety threats and develop provisions to support there increased vulnerability.

Consider alternative ways to further educate and support online safety provision for parents and carers, investigate remote learning material that could make training more accessible for the whole school community

GRADE: 4.5

2. Governance

Governance

This aspect reviews process in place and involvement of governors/trustees within how online safety provision is embedded within the school. Evidence could include Minutes of governors meetings, stakeholder survey, school council or online learning group initiatives, governor allocations, sharing of best practice and self evaluative measures.

LEARNERS

A school council is in place that is consulted upon policy change and acts as a platform for raising concerns of a safeguarding and online safety nature. This could be leveraged further and could include the use of learners from the school council to run an INSET session onto their use of social media and the internet to give a deeper insight for educational practitioners.

STAFF

A governor is assigned to Safeguarding which encompasses a responsibility for online safety. Online Safety incidents are reported to governors alongside safeguarding information at all meetings. Governors have an involvement in the development of online safety policy.

COMMUNITY

No parents/carers are involved in online safety initiatives within the school although most parents are contacted daily and concerns are fed back into whole school planning and provision for online safety.

Suggested Actions for Improvement:

Use the school council to gain insight into current concerns of the school population which can then be used to tailor learning.

Develop a more thorough Online Safety group to run alongside the school council. Learners form all year groups should be involved alongside parents, teachers and teachers.

GRADE: 4.5

3. Policy and Process

Policy and Process

This aspect investigates and reviews currently implemented policies and process that are in place for reporting, acting upon a concern and how data and stakeholders are used to drive policy review Evidence could include policies, organisational process flowcharts, data analysis, Stakeholder survey, clear routes of reporting for all stakeholders and policy review schedule.

REPORTING

Report of online safety concerns and incidents can be easily made through a range of methods. The nature of the school means that teachers work very closely with parents, talking daily where possible. This provides an excellent route for parents to report. A high staff to student ratio means that staff build stronger relationships with learners than a normal school environment making it easier for learners to report. Teachers report through set process and safeguarding meetings.

POLICIES

The school has an online safety policy, where roles are clearly defined. It is effective and meets the school's safeguarding obligations. It has been developed in consultation with a wide range of staff and pupils / students. There is “whole school ownership” of the policy. The policy is reviewed annually.

PROCESS

A clear process has been defined for dealing with all safeguarding and online safety concerns and incidents. This is detailed in the schools safeguarding policy which references other supporting policies.

SELF EVALUATION

Whole school ownership is a key focus of all policy development and all stakeholders are consulted on new policies and feedback used to refine them. Presently safeguarding data is not used to inform policy change or identify trends.

Policy and Process

This aspect investigates and reviews currently implemented policies and process that are in place for reporting, acting upon a concern and how data and stakeholders are used to drive policy review Evidence could include policies, organisational process flowcharts, data analysis, Stakeholder survey, clear routes of reporting for all stakeholders and policy review schedule.

Suggested Actions for improvement

Develop systems of tracking and analysis to allow for frequent review (if required by incidents or developments in new technologies).

Use safeguarding data to inform future Online Safety policy development.

GRADE: 4

4. Communication & Communications Technologies

Communication & Communications Technologies

This aspect investigates and reviews the use of technology within the educational environment; The use of devices, social media and general communications. Evidence could include organisational communication policies and procedures, social media policies, home/school agreements, documented social media accounts, BYOD policy, IT infrastructure development plans.

Bring Your Own Device (BYOD)
A policy is in place to restrict the use of personal devices within the school.

Use of Technology
A range of technology is available within the school including a well equipped ICT suite and laptops in classrooms. All devices use schools filtering which is controlled via head office.

Social Media and Lines of Communication
Policies are in place making staff aware of their professional responsibilities when using social media. Clear communication routes are in place and staff communicate daily with parents and carers.

Policies and Process
The school understands the potential damage that social media can have upon the school as an organisation and the educational practitioners that it employs, in light of which the school has begun to implement appropriate responses where necessary.

Suggested Actions for Improvement:

Continue to investigate the best practice uses of technology and social media in the school environment to ensure that technology is leveraged to its full potential.

Promote apps and social media in a positive way to identify learning tools/apps and highlight the potential positive impact of technology as well as the risks to online safety.

GRADE: 4

5. Infrastructure

Infrastructure

As part of the infrastructure section we review the technological measures that are being taken to ensure the safety of stakeholders. This includes, filtering and monitoring; Evidence could include Acceptable use policies, password policies, robust filtering and monitoring, analysis of filtering data, backup strategy, data protection policies, disaster recovery polices and penetration testing reports.

PHYSICAL SECURITY

Servers are stored in a secure room with restricted access to only those that need it. All IT services are provided by the local authority and backed up to county hall using a dedicated line. Password polices follow Windows minimum standards for security and dual factor authentication is used to access safeguarding systems.

LOGICAL SECURITY

Anti-virus, Malware and filtering are all in place, managed by the LA and utilise Sophos software solutions. Filtering does not provide automatic notifications to the DSL and Online Safety lead. Where filtering and monitoring do flag an issue, positive intervention is established for the involved learners.

BACKUPS & DATA PROTECTION AND RETENTION

Backups are all carried out remotely by the local authority. A disaster recovery plan is in place. The school employs a full time data manager who has created stringent process to ensure organisational level compliance with the Data Protection Acct. The school is fully aware of GDPR and forthcoming regulations and is in the process of attending courses and developing a roadmap to achieve GDPR compliance

Infrastructure

As part of the infrastructure section we review the technological measures that are being taken to ensure the safety of stakeholders. This includes, filtering and monitoring; Evidence could include Acceptable use policies, password policies, robust filtering and monitoring, analysis of filtering data, backup strategy, data protection policies, disaster recovery polices and penetration testing reports.

Suggested Actions for Improvement:

Work closely with your filtering and monitoring provider to establish a route to automatically notify the DSL and Online Safety lead of potential Online Safety/Prevent issues that need to be addressed and fed back into safeguarding data to inform policy development and change.

Consider the implementation of a full penetration test at county hall level to ensure that all servers are fully secure and unused ports are all closed

Continue to work towards GDPR compliance ready for the 25th May 2018.

GRADE: 4