Chester Park Federation Online Safety Policy

Approved by:	Policy Working Group	**Date:** June 2020
Last reviewed on:	5th February 2024	
Next review due by:	February 2025	

This Online Safety policy has been developed by a working group made up of:

- Headteacher
- Online Safety Officer / Computing Co-ordinators
- Staff – including Teachers, Support Staff, Technical staff
- Governors
- Parents and Carers

Consultation with the whole school community has taken place through a range of formal and informal meetings.

This policy has been developed in line with Keeping Children Safe in Education 2023

Schedule for Development / Monitoring / Review

This Online Safety policy was approved by Governors Sub Committee on:	*June 2020*
The implementation of this Online Safety policy will be monitored by the:	*Computing lead* *SLT team*
Monitoring will take place at regular intervals:	*Yearly*
The Governing Body will receive a report on the implementation of the Online Safety Policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place.	
Should serious online safety incidents take place, the following external persons / agencies should be informed:	*LA, LADO, Social Care, First Response, Police*

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited) / filtering
- Internal monitoring data for network activity
- Surveys / questionnaires of
    - students / pupils
    - parents / carers
    - staff

Scope of the Policy

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

Technical – infrastructure/equipment filtering and monitoring

The Federation supported by the LA and 'Soltech' technicians will be responsible for ensuring the school infrastructure/network is safe and secure as reasonably possible and that policies and procedures approved within the Online Safety Policy are implemented.

Incident Management

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other Online Safety 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.

Chester Park Infant School and **Chester Park Junior School** will deal with such incidents within this policy and associated behaviour, anti-bullying and prevent policies and will, where known, inform parents / carers of incidents of inappropriate Online Safety behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the federation:

Governors:

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the *Governors* receiving regular information about online safety incidents and monitoring reports. A member of the *Governing Body* has taken on the role of *Online Safety Governor* (the role is combined with that of the Child Protection / Safeguarding Governor). The role of the Online Safety *Governor* will include:

- regular meetings with the Computing Co-ordinators
- attendance at Online Safety Group meetings
- regular monitoring of online safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Governors

Headteacher and Senior Leaders:

- The *Headteacher* 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 Co-ordinator*.
- The Headteacher and (at least) another member of the Senior Leadership Team 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.
- The Headteacher /Senior Leaders are responsible for ensuring that the Computing Co-ordinators 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 Headteacher/ 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 Computing Co-ordinators.

Computing (Online Safety) Co-ordinators:

- leads the Online Safety Group
- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority / relevant body
- liaises with school technical staff
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments
- meets regularly with Online Safety *Governor* to discuss current issues, review incident logs and filtering / change control logs
- attends relevant meeting / committee of *Governors*
- reports regularly to Senior Leadership Team

Network / Technical support staff:

The Network Manager / Technical Staff is responsible for ensuring:

- that the *federation's* technical infrastructure is secure and is not open to misuse or malicious attack
- that the federation meets required online safety technical requirements and any *Local Authority* Online Safety Policy / Guidance that may apply.

- 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
- Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet.
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the *network / internet / remote access / email* is regularly monitored in order that any misuse / attempted misuse can be reported to the *Headteacher /Online Safety Coordinator* for investigation / action / sanction
- that monitoring software/ systems are implemented and updated as agreed in federation/school policies

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current federation Online 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/ Online Safety Coordinator for investigation / action / sanction
- all digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official school systems
- online safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the Online Safety Policy and acceptable use policies
- pupils 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
- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- staff with access to personal data must know, understand and adhere to the relevant policy which brings together the statutory requirements contained in relevant data protection legislation, regulations and guidance (GDPR).

Designated Safeguarding Lead

Should be trained in Online Safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

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

Online Safety Group

The Online Safety Group provides a consultative group that has wide representation from the federation community, with responsibility for issues regarding online safety and the monitoring the Online Safety Policy including the impact of initiatives. The group will also be responsible for regular reporting to the *Governing Body*.

Members of the Online Safety Group will assist the Computing Co-ordinators with:

- the production / review / monitoring of the federation Online Safety Policy / documents.
- the production / review / monitoring of the school filtering policy
- mapping and reviewing the online safety curricular provision – ensuring relevance, breadth and progression
- monitoring network / internet / incident logs
- consulting stakeholders – including parents / carers and the students / pupils about the online safety provision
- monitoring improvement actions identified through use of the 360 degree safe self-review tool

Pupils:

- are responsible for using the federation digital technology systems in accordance with the Pupil Acceptable Use Agreement
- 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 online safety practice when using digital technologies out of school and realise that the federation*'s* Online Safety Policy covers their actions out of school, if related to their membership of the school

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. **Chester Park Infant School and Chester**

Park Junior School will take every opportunity to help parents understand these issues through *parent consultation evenings, newsletters, letters, website and information about national / local online safety campaigns / literature.* Parents and carers will be encouraged to support the federation in promoting good online 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
- their children's personal devices in the school

Community Users

Community users who access school systems/websites as part of the wider school provision will be expected o sign a Community User AUA before being provided with access to school systems.

Acknowledgements

SWGfL would like to acknowledge a range of individuals and organisations whose policies, documents, advice and guidance have contributed to the development of this School Online Safety Policy Template and of the 360-degree safe Online Safety Self Review Tool:

- Members of the SWGfL Online Safety Group
- Avon and Somerset Police
- Representatives of SW Local Authorities
- Plymouth University Online Safety
- NEN / Regional Broadband Grids