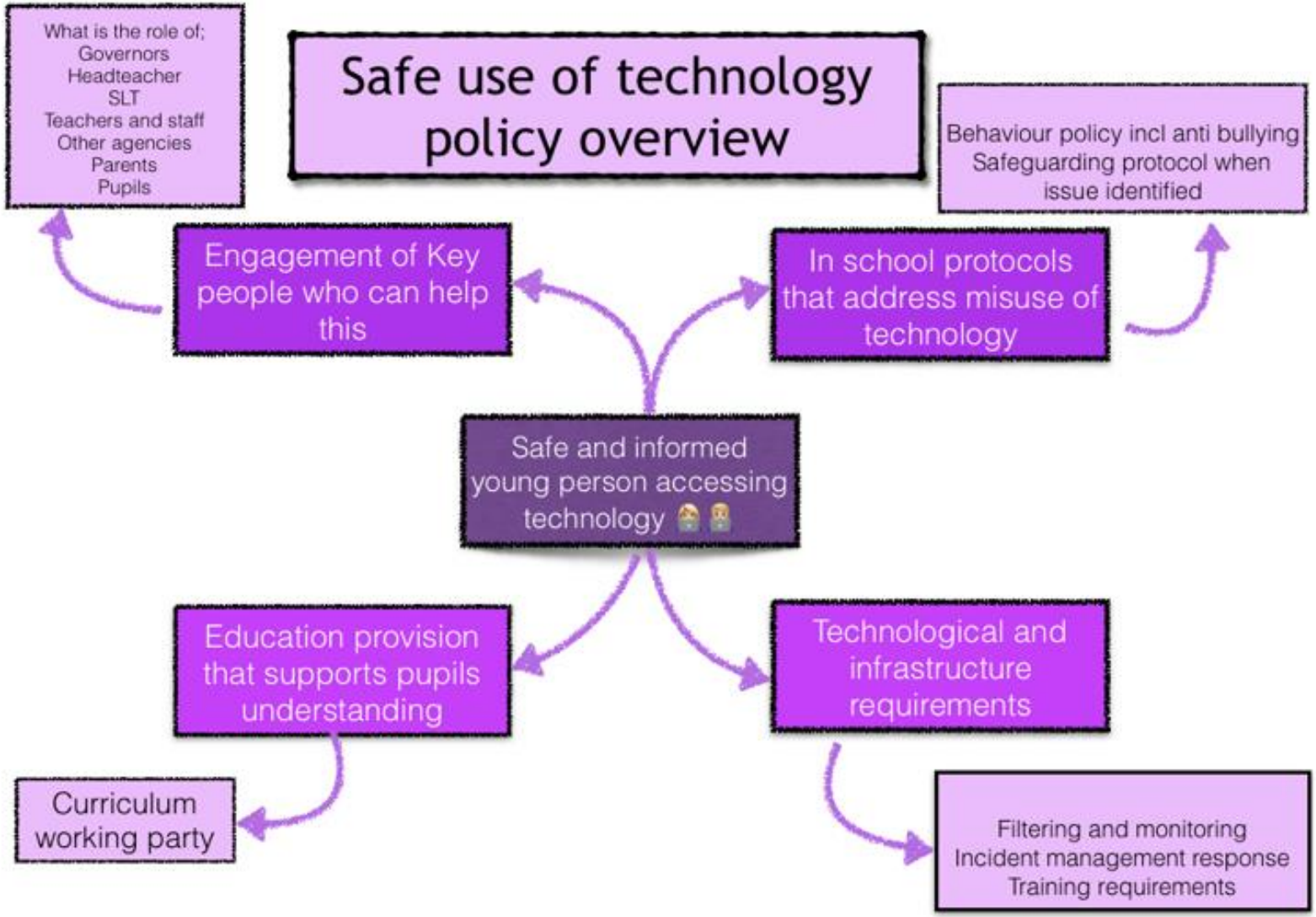
Online Safety Policy

Date of last review:	2017	**Review period:**	2 Years
Date of next review:	2019	**Written by:**	Brian Thomas
Type of policy:	Non-statutory	**Committee:**	Curriculum & Standards
Signature:			


Safe use of technology policy overview
What is the role of;
Governors
Headteacher
SLT
Teachers and staff
Other agencies
Parents
Pupils
Behaviour policy incl anti bullying
Safeguarding protocol when issue identified
Engagement of Key people who can help this
In school protocols that address misuse of technology
Safe and informed young person accessing technology
Education provision that supports pupils understanding
Technological and infrastructure requirements
Curriculum working party
Filtering and monitoring
Incident management response
Training requirements

Wyre Forest School recognise the importance of ensuring that our pupils are safeguarded in their use of technology within school, particularly relating to the use of the internet and online safety. We adopt a pro-active and rigorous approach to monitor the use of technology and staff are required to report any instances of misuse to the Designated Safeguarding Lead and the Network Manager. We recognise that there is an increased vulnerability associated with pupils with SEN accessing online materials and all staff have a duty to ensure all pupils access to technology and online materials is monitored rigorously.

We also need to ensure that we work closely with parents/carers and other agencies to create a wrap-around approach that keeps all of our pupils safe when using technology.

Unfortunately, despite all of our efforts there will always be occasions when inappropriate use of technology does happen and a pupils safeguarding is compromised and we need to be clear on the protocols to follow in these situations.

Examples of these situations include, but are not limited to, the following:

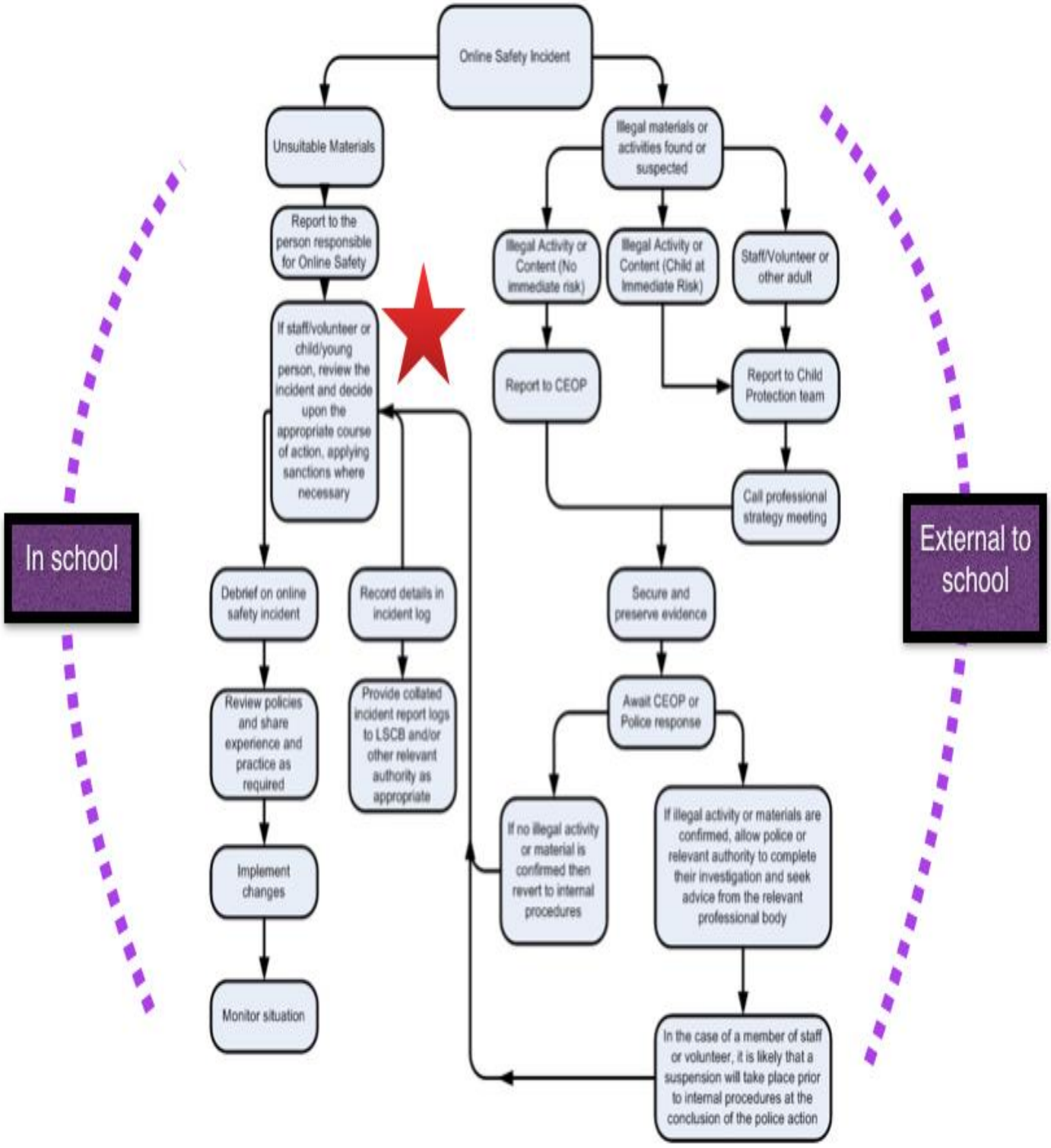
- Accessing inappropriate material online, be it directly or indirectly, e.g. pornographic, racist, homophobic, radicalisation, etc. This can include websites, chat rooms, social media, etc.

- Using technology to bully or abuse others, e.g. making negative comments on social media, taking photographs of others without permission, using photographs inappropriately, etc.

- Sharing information with others online that increases a young person's vulnerability.

- Suggesting or intimating that they access inappropriate materials as highlighted above.

It is important that this misuse is addressed immediately and then monitored regularly to ensure that the risk of repetition is removed or reduced significantly and we ask staff to adhere to the following protocol for any situation when misuse of technology is identified:


Online Safety Incident
Unsuitable Materials
Illegal materials or activities found or suspected
Report to the person responsible for Online Safety
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
In school
External to school
Debrief on online safety incident
Record details in incident log
Secure and preserve evidence
Review policies and share experience and practice as required
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Await CEOP or Police response
Implement changes
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
Monitor situation
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action

Wyre Forest School Increase in Severity of Response Dependent on the Nature of Incident

Wyre Forest School recognise that there will be occasions when pupils do contravene the Online Safety Policy and will require immediate follow up to remedy this. Please find below our processes for responding to breaches to the Online Safety Policy.

Nature of Incident	School Response	Follow-up and Monitoring
Pupil accesses inappropriate material either unknowingly or with little consequential awareness of the impact of the material	DSL and Network Manager informed Report to Pastoral Team Parents/carers contacted and incident discussed Device confiscated to allow inappropriate material to be removed and consider temporary ban on accessing technology independently	Daily device checks completed by Class Teacher/Key Worker and weekly update to Network Manager required
Pupil accesses inappropriate material knowingly	DSL and Network Manager informed Report to Social Services Report to Pastoral Team Parents/carers contacted and incident discussed All devices removed from young person until an access strategy is agreed involving school, parents/carers and any other agencies involved	Daily device checks completed by Class Teacher/Key Worker and weekly update to Network Manager required

Pupil uses technology to bully or belittle others	DSL and Network Manager informed Report to Social Services Report to Pastoral Team Parents/carers contacted and incident discussed All devices removed from young person until an access strategy is agreed involving school, parents/carers and any other agencies involved	Remove devices immediately and complete technology access strategy Daily device checks completed by Class Teacher/Key Worker and weekly update to Network Manager required
Illegal material accessed knowingly	Follow the right-hand side of the protocol above including police involvement	See protocol on flow chart

Please note:

Wyre Forest School have an open and empathetic culture surrounding behaviour and work hard to involve pupils in discussions and education about appropriateness of behaviour and self-regulation. It is often the case that the above responses can be implemented with the support of the young person and HAVE to be implemented with the FULL support and commitment to address the issue from parents/carers.

Roles and Responsibilities of People Involved in Ensuring Pupils are Safe Online:

The following section outlines the online safety roles and responsibilities of individuals and groups within Wyre Forest School.

Governors:

The Wyre Forest School Governing Body 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 Wyre Forest School Governing Body receiving regular information about online safety incidents and monitoring reports. This will be part of our school Safeguarding Monitoring Schedule. Our named Governor for safeguarding and also safe use of technology is Jeffrey Howell. He will meet regularly with the Safeguarding Leads and monitor issues surrounding safe use of technology.

Headteacher and the Senior Leadership Team:

- The Headteacher has a duty of care for ensuring the safety of members of the school community and will respond to every breach of the Online Safety Policy

and take appropriate action as stated in the Online Safety Policy.

- The Headteacher and 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 (refer to flow chart on dealing with online safety incidents – included in a later section – "Responding to incidents of misuse" and relevant *Local Authority HR* disciplinary procedures).

- The Headteacher will meet on a weekly basis with the Safeguarding Team where any issues involving the use of technology will be discussed and actions agreed.

Safe Use of Technology Monitoring Lead:

The Designated Safeguarding Lead will also monitor the safe use of technology within the school. This will happen in conjunction with the school Educational Technologist who has the knowledge required and access to the school monitoring systems for the safer use of technology.

Network Manager/Technical Staff:

The school based Educational Technologist 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 online safety technical requirements and any Local Authority and other relevant body 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 (if it has one) 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 IB – exclusion 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/Learning Platform/remote access/email is regularly monitored in order that any misuse/attempted misuse can be reported to the Designated Safeguarding Lead;

- that monitoring software/systems are implemented and updated as agreed in school/academy policies.

Teachers, Teaching Assistants and Support Staff:

Teachers, TAs and Support Staff are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current school Online Safety Policy and practices;
- they have read, understood and signed the Staff Acceptable Use Policy (AUP);
- they report any suspected misuse or problems to the Designated Safeguarding Lead 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 Safe Use of Technology Policy and Acceptable Use Policy;
- 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, students/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.

Designated Safeguarding Lead:

The 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:

- the sharing of personal data;
- access to illegal/inappropriate materials;
- inappropriate online contact with adults/strangers;
- potential or actual incidents of grooming;
- cyber-bullying.

Pupils:

- are responsible for using Wyre Forest School digital technology systems in accordance with the Pupil Acceptable Use Agreement;
- need to understand that the internet is a dangerous place and it is important to report any abuse, misuse or access to inappropriate materials and know how to do so;

- will be expected to know what is appropriate and inappropriate 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 Wyre Forest Schools' Safe Use of Technology 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. Wyre Forest School will take every opportunity to help parents/carers understand these issues through *Parents' Evenings, newsletters, letters and the school website*, and will share information about national/local online safety campaigns. Parents/carers will be encouraged to support Wyre Forest School 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 and online pupil records;

- their children's personal devices in Wyre Forest School (where this is allowed).

Community Users:

Community users who access school systems/website as part of the wider school provision will be expected to sign a Community User Acceptable Use Agreement before being provided with access to school systems.

Pupils require a complete 'wrap around' approach in order to educate them about the benefits, and also dangers, of using technology; and also, adults need to act in a 'guardian' capacity to identify when pupils are at risk of being exploited with their use of technology and the internet.

Wyre Forest School Training Expectations of Staff

Staff Training and Education – General

Wyre Forest School link with the Virtual College to provide a range of training packages that support the needs of staff and pupils. It is compulsory for all staff to access online safety training through the Virtual College and in addition the school will carry out a 'use of technology' audit at least once per year to identify specific training needs of staff and this will inform our performance management process. New staff will receive online safety training as part of their induction programme. In addition, Wyre Forest School receive training from Apple accredited trainers in the use of Apple computers and technologies. Staff are encouraged to develop their understanding of technology and ensure that they are aware of how to be online

smart.

Staff Training and Education – Specifics

Identified staff (currently the Network Manager and Safeguarding Leads) will access external events and training opportunities that enhance their knowledge of safe use of technology. This will then be disseminated to staff in the school and parents/carers (where relevant). Identified staff may also access this training.

Staff Training and Education – Governors

Governors will access safe use of technology training by using the Virtual College training package. Governors directly involved in online safety or safeguarding work should receive additional training through the following methods:

- Attendance at training provided by the Local Authority/National Governors Association/or other relevant organisations (e.g. SWGfL).

- Participation in school training/information sessions for staff or parents/carers (this may include attendance at assemblies/lessons).

Wyre Forest School Technical Expectations including Filtering and Monitoring

Technical – Infrastructure/Equipment, Filtering and Monitoring

Wyre Forest School will be responsible for ensuring that our school infrastructure and 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 online safety responsibilities:

- Wyre Forest School technical systems will be managed in ways that ensure that we meet recommended technical requirements.

- Wyre Forest School will have regular reviews and audits of the safety and security of our 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 at Key Stage 3 and above will be provided with a username and secure password by Steve Cronin who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password.

- “Administrator” passwords for the school ICT system, used by the Network

Manager (or other person), must also be available to the Headteacher or other nominated Senior Leader and kept in a secure place (e.g. school safe).

- Steve Cronin 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 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. Wyre Forest School has a clear process in place to deal with requests for filtering changes and for occasions when the filtering identifies an issue.

- Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet. A record of any instances of inappropriate material will be kept by the Safeguarding Team. Wyre Forest School has provided enhanced/differentiated user-level filtering (allowing different filtering levels for different ages/stages and different groups of users – staff/pupils/students, etc.)

- Wyre Forest School 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.

- An appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person, as agreed.

- 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. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.

- An agreed policy will be in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school systems (in place by January 2018).

- 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.

Related Policies:

- Behaviour Policy

- Data Protection Policy
- Safeguarding (including Child Protection) Policy
- ICT Disaster Recovery Plan