The Ryedale Federation

e-Safety Policy

Policy Review Timescales:	Annual
Review Committee:	Secondary Director/Headteacher
Last updated:	September 2019
Review Date:	July 2020

Introduction and Aims

Background information

New technologies have become integral to the lives of children and young people in today's society, both within educational establishments and in their lives outside school. The internet and other digital/information technologies are powerful tools which open up new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

Keeping Children Safe in Education (September 2019) clearly states that, '*The use of technology has become a significant component of many safeguarding issues. Technology often provides the platform that facilitates harm. An effective approach to online safety empowers a school to protect and educate the whole school in their use of technology and establishes mechanisms to identify intervene and escalate any incident where appropriate':*
https://www.gov.uk/government/publications/keeping-children-safe-in-education--2

The requirement to ensure that children and young people are able to use the Internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. This e-safety policy will help to ensure safe and appropriate use. The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement. However, the use of these new technologies can put young people at risk within and outside the school.

The breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk:

- Content: being exposed to illegal, inappropriate or harmful material
- Contact: being subjected to harmful online interaction with other users
- Conduct: personal online behaviour that increases the likelihood of, or causes, harm

Some of the risks students face include:

- Access to illegal, harmful or inappropriate images or other content (including radicalisation /extremism material and pornography)
- Unauthorised access to, loss of or sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the Internet.
- The sharing/distribution of personal images with and without an individual's consent or knowledge
- Inappropriate communication/contact with others, including strangers

- Cyber-bullying
- Access to unsuitable video/Internet games/ websites
- An inability to evaluate the quality, accuracy and relevance of information on the Internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person
- Generating large bills through overuse of their mobiles, gaming etc

Online Safety Policy

The Ryedale Federation's online safety policy to be read and used in conjunction with other school policies; specifically the anti-bullying, information (data protection) policy, behaviour, child protection / safeguarding, relationships and sex education and a clear understanding on the use of personal mobile technology in the school. Many pupils have unlimited and unrestricted access to the internet via 3G and 4G in particular; The Ryedale Federation gives careful consideration how this is managed on the schools' premises.

This online safety policy has been developed through wide consultation with the whole school community and takes into account all the key aspects identified in this guidance document.

Who this policy applies to:

- All members of the school and setting community (including staff, pupils, governors, volunteers, parents/carers and visitors) who have access to and are users of school ICT systems, both in and out of school, as well as use of personal technology whilst on the school premises or engaged in school activities.
- The Education and Inspections Act 2006 empowers the Headteacher/Secondary Director/Head of School 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 cyber-bullying or other online safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school. The school should deal with such incidents within the procedures set out in the online policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that takes place out of school.

Please see useful links to further guidance below:

- Safer internet .org.uk http://www.saferinternet.org.uk/advice-and-resources/teachers-and- professionals/esafety-policy
- Esafety adviser http://www.esafety-adviser.com/resources/

Roles & Responsibilities

This section outlines the roles and responsibilities for online safety of individuals and groups within the federation schools.

Roles & Responsibilities of Governors:

Governors are responsible for the approval of the online safety policy, ensuring it is dis-seminated to the wider school community and for reviewing the effectiveness of the policy. Mr David Dangerfield, Chair of Governors for The Ryedale Federation, takes on our school's role of online safety governor and has accessed training about online safety. The role of the governing board does include:

- Ensuring that the statutory requirements of Keeping Children Safe in Education (Sept' 2019) are complied with. In relation to online safety this includes:

- Ensuring that as part of the requirement for staff to undergo regularly updated safeguarding training and the requirement to ensure children are taught about safeguarding, including online that online safety training for staff is integrated, aligned and considered as part of the overarching safeguarding approach.

- Ensuring that pupils are taught about safeguarding, including online, through teaching and learning opportunities, as part of providing a broad and balanced curriculum. This may include covering relevant issues through PSHE.
- As schools increasingly work online it is essential that students are safeguarded from potentially harmful and inappropriate online material. The Ryedale Federation Schools aim to ensure the appropriateness of any filters, monitoring and security systems which will be informed in part by the risk assessment required by the Prevent Duty to ensure that students are safe from terrorist and extremist material whilst accessing the material in school, including by establishing appropriate levels of filtering but being careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding'.
- Regular monitoring of online safety incident logs and responding appropriately to the identified needs.
- Ensure the schools' websites host has enough security in place so it cannot be inappropriately accessed and to have an action plan if it is 'hacked' e.g, who regularly checks the website including during school holidays and, who is the key contact if the website is hacked.
- The UKCCIS Education Group has developed guidance for school governors to help governing boards support their school leaders to keep children safe online which can be accessed at: https://www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis

Further support on appropriate filtering and monitoring

The UK Safer Internet Centre has published guidance as to what "appropriate" filtering and monitoring might look like both for schools/ settings and for providers of internet services in schools. These documents will provide a useful checklist when a school reviews the appropriateness of their present systems. All documents can be accessed from UK Safer Internet Centre:

http://www.saferinternet.org.uk/advice-and-resources/teachers-and- professionals/appropriate-filtering-and-monitoring.

Guidance on e-security is available from the National Education Network-NEN. http://www.nen.gov.uk/

The Ryedale Federation may use recommended resources:

Support for schools to review their online safety policy and practice via the 360 degree safe self-review tool, free to use and provides:

- Information that can influence the production or review of e-safety policies and develop good practice
- A process for identifying strengths and weaknesses
- Opportunities for commitment and involvement from the whole school
- A continuum for schools to discuss how they might move from a basic level provision for online safety to practice that is aspirational and innovative.

https://360safe.org.uk/About-the-Tool

A resource to support Early Years setting review their policy and practice is available at

https://kentesafety.wordpress.com/2017/09/05/updated-kent-online-safety-policy-template-and-guidance-esafety/amp/

The Governors and Headteacher/Secondary Director/Heads of School need to ensure that the online safety policy is crossed referenced with the Information Policy (data protection) with particular reference to nobody taking data outside of the school system and complies with GDPR. The policy needs to consider

how information is shared/accessed with the governing body for example all governors being issued with a school email address, accessing information through a shared 'storage cloud', or on a secure part of the school's website or being provided with an encrypted memory stick. These systems need to be agreed and adhered to by all governors. It is recommended that all governors sign an acceptable use policy (see appendix 6 for model AUP). Further information for governors about information governance can be accessed at http://cyps.northyorks.gov.uk/information- governance-schools

Roles & Responsibilities of the Headteacher/Secondary Director:

- Supporting the Governors comply with the online safety aspects of the Keeping Children Safe in Education, September 2019 documentation
- The safety (including online safety) of all members of the school community.
- Effective and regular training about online safety is provided for the whole school community and a log is kept of the staff who complete the training
- Governors are invited to take part in online safety training and awareness sessions, with particular importance for those who are members of any committee or working group involved in ICT, online safety education, health and safety or child protection.
- Effective communication with parents/ carers about safe practices when using online technology's and support them in talking to their children about these issues
- Effective filtering, monitoring and security systems are set up
- There are effective procedures in place the event of an online safety allegation which are known and understood by all members of staff
- Establishing and reviewing the school online safety policy and documents and making them available on the school website
- The federation school's Designated Safeguarding Lead should be trained in online safety issues and be aware of the potential for serious child protection issues that could arise through the use of ICT.

Roles & Responsibilities of a named member of the Senior Leadership Team:

At Helmsley CP School:
Mrs Clare Lamb, Head of School & DSL / Nicola Dunn, Deputy DSL

At Kirkbymoorside CP School:
Mrs Gill Hardacre, Primary Director and DSL and Gareth Sleightholme, Head of School and Deputy DSL

At Ryedale School:
Domenica Wilkinson, Secondary Director & DSL / Carolyn Williams, Assistant Headteacher and Deputy DSL

At Sinnington CP School:
Neil Roden, Head of School / Gill Hardacre, Primary Director and DSLs and Helen Thompson, Deputy DSL

- Liaising with staff, ICT Technical staff, online safety governor, SLT and partner agencies on all issues related to online safety
- Ensuring that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place
- Providing training and advice for staff and keeping a log of staff who complete training about online issues
- Keep a log of staff, students and families who have signed the Acceptable Use Policy (AUP) for the safe use of technology
- Receive and respond to reports of online safety incidents and create a log of incidents and outcomes

to inform future online safety developments
- Co-ordinating and reviewing online safety education programme in school (or working in partnership with the Personal, Social, Health, Education (PSHE) and/ or Computing lead).

Roles & Responsibilities of the ICT technician:

At Helmsley CP School:
Mr Simon Hadden, Network Manager

At Kirkbymoorside CP School:
Mr Steve Chandler (SMD Ltd), Network Manager

At Ryedale School:
Mr Simon Hadden, Network Manager

At Sinnington CP School:
Mr Simon Hadden, Network Manager

- The Ryedale Federation's ICT infrastructure is secure and meets requirements for filtering and monitoring
- The Ryedale Federation's websites are kept secure from 'hacking' and there is an action plan in place if it is hacked
- The Ryedale Federation's passwords policy is adhered to
- The Ryedale Federation's filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- The Ryedale Federation keeps up to date with online safety technical information
- The use of the federation schools ICT infrastructure (network, remote access, e-mail, VLE etc.) is regularly monitored in order that any misuse or attempted misuse can be reported to the named SLT for action.

Roles & Responsibilities of all staff:
In addition to the elements covered in the Staff Acceptable Use Policy (AUP), all Ryedale Federation school staff are responsible for ensuring that:
- They have an up to date awareness of online safety matters and of their school's current online safety policy and practices
- They attend the training provided by the school about online safety and all new staff receive online safety training as part of their induction programme, ensuring that they fully understand the school's online safety policy, Acceptable Usage and Child Protection Policies
- They have read, understood and signed the school Staff Acceptable Usage Policy (AUP)
- They do not 'be-friend' any student or student family member on social media in a social context as a result of their position in the school
- Online safety issues are embedded in all aspects of the curriculum and other school activities
- Students understand and follow the school's online safety and acceptable usage policies
- Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They monitor ICT activity in lessons, extracurricular and extended school activities
- In lessons where Internet use is pre-planned, students 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

- All staff should be aware that emails can be part of Freedom of Information requests so all correspondence needs to be professional, courtesy and respectful

- If confidential information / information under the data protection act is being sent by email it must be sent through a secure email system which the school's administration and Headteacher/Secondary Director/Head of School have access to but more licenses can be purchased.

Safer Internet have produced various supporting guidance and documents for staff who work in schools to enable them to help young people to stay safe online but also to ensure they protect their own online reputation, particularly when using social networking sites. http://www.saferinternet.org.uk/advice-and-resources/teachers-and-professionals

Roles & Responsibilities of all students

- Are responsible for using the federation school's ICT systems in accordance with the Pupil Acceptable Usage Policy, which they will be required to sign before being given access to school systems. Parents/carers will be required to read through and sign alongside their child's signature.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's online safety policy also covers their actions out of school, if related to their membership of the school or using equipment provided by the school.

Roles & Responsibilities of all 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. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The Ryedale Federation will therefore take opportunities to help parents understand these issues. Parents and carers will be responsible for:

- Endorsing (by signature) the Pupil Acceptable Usage Policy and will alongside this sign the Parents/ Carers Acceptable Usage Policy
- Access the school website and correspond with the school in accordance with the Parents Acceptable Usage Policy.
- Ensuring that they do not use social media to criticise or make inappropriate comments about the Ryedale Federation schools or an individual member of staff as making defamatory comments online has exactly the same legal consequences as if they are made directly to someone else. Similarly, threats of violence can lead to criminal proceedings under the Malicious Communications Act. If as a parent/ carer you have any concerns about anything which happens in school then please contact us directly on 01439 771665.

Parents and Carers should also be aware of the health effects of children and young people having too much 'screen time'. This can limit the amount of time children are being physically active, reduce the amount of time they are sleeping and could be impacting on their eyesight. A number of systems and apps are available that can limit the screen time for students alongside parents and carers talking to their children about the issues.

The following websites ***(see overleaf)*** provide supporting information for parents / carers to enable them to protect their children through setting up parental controls and being able to talk to their children about how to stay safe online. This information on page 11, forms part of our e-Safety policy which is available on the school website for parents/ carers to access.

NSPCC online safety https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/	Provides helpful advice and tools that a parent/carer can use to help keep their child safe whenever and wherever they go online. • Has material and information for use with young children as well as older children • Key advice for parents / carers • Information on a range of social media sites and games
Thinkuknow https://www.thinkuknow.co.uk/parents/	Provides helpful advice and tools that a parent/carer can use to help keep their child safe online. Downloadable guides for parents/ carers on various social media sites like: Instagram, Whatsapp, youtube etc They also have some useful films for parents to watch about the risks online and four specific films about sexting / 'self nudies' and how to talk to their children about this issue and what to do if this happens.
Childnet http://www.childnet.com/parents-and- carers The whole website can be read in a variety of languages.	A range of information to support parents/ carers keep their children on safe including: • Parents: Supporting Young People Online (Leaflets in a variety of languages) • Key advice for parents / carers • Conversation starters to enable parents /carers to talk to their children • How to set parental controls on a range of devices • Gaming
Safer internet http://www.saferinternet.org.uk/advice- and-resources/parents-and-carers	Very specific advice, films and signposting to ensure parents/ carers have the information about how to set up parental controls on a range of devices and their home internet
Internet matters https://www.internetmatters.org/advice/	Provides a wealth of information for parents/ carers on internet safety starting for parents and carers of 0-5 year olds working upwards. Information, films and advice about parental settings and information about a range of games and apps that are popular with children and young people to help parents make informed decisions
North Yorkshire Local Children Safeguarding Board (LCSB) http://www.safeguardingchildren.co.uk/parents-and-carers	In partnership with other agencies the LSCB have developed an information leaflet containing practical advice about how parents/ carers can support their children stay safe online

Staff training opportunities

It is important that staff are kept up-to-date with online safety issues for children and young people but also for them to consider their online presence.

Training is available through the Education and Skills team (NYCC) and the team has a trained CEOP ambassador (there is a cost for attending this training):

- NYCC Online safety in primary schools and settings: meeting your statutory safeguarding duties
- NYCC Online safety in secondary schools / PRS: meeting your statutory safeguarding duties
- A twilight/ staff training day version of this NYCC training can be delivered in a school / to a cluster of schools for staff and/ or governor training which can also be purchased alongside an awareness session for parents / carers.

To book the following NYCC provided training through North Yorkshire Education Services
www.nyeducationservices.co.uk

- CEOP provide face-to-face training events. They only train DBS (or equivalent) cleared professionals who will directly deliver CEOP's (think u know) products and resources to children. https://www.thinkuknow.co.uk/Teachers/Training/

- Mind Ed – provide free online training focused on:
    - Online Risk And Resilience
    - Digital Media and Young People
    - Children and Young People's Digital Lives

https://www.minded.org.uk/local/search/search_programs

- An online safety INSET presentation that has been designed to be delivered by the online safety Lead, or designated staff member, in a school, organisation or child care setting.

http://www.childnet.com/teachers-and-professionals/staff-e-safety-inset-presentation

- NSPCC- Keeping children safe online is a 3 hour online course, £20 per person
    - how children use the internet and technology
    - the risks they face from other people - both other children and adult offenders
    - behaviour by children that exposes them to greater risks online
    - what to do if children experience issues such as cyber bullying or grooming
    - how to make organisations safer places for children to go online
    - how to conduct an e-safety audit and create an acceptable use policy for your organisation.

https://www.nspcc.org.uk/what-you-can-do/get-expert-training/keeping-children-safe-online-course/

Online safety curriculum for students that is age appropriate and is a well-planned and taught curriculum

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision, to build students' resilience to the risks to which they may be exposed so that they have the confidence and skills to face and deal with these risks.

The Ryedale Federation aims to provide the necessary safeguards to help ensure that they have done everything that could reasonably be expected to manage and reduce these risks. The online safety policy explains how the school intends to do this, whilst also addressing wider educational issues in order to help young people (and their parents/carers/staff) to be responsible users and stay safe while using the Internet and other communications technologies for educational, personal and recreational use.

The Government has announced that Relationships and Sex Education and Health Education will become statutory for all schools in September 2020. The draft Relationships Education, Relationships and Sex Education and Health Education guidance has been consulted upon in 2018. The draft guidance and information can be accessed at https://consult.education.gov.uk/pshe/relationships-education-rse-health-education/ . It is recommended that schools start to plan for these statutory requirements before September 2020. The government want pupils to be able, "to embrace the challenges of creating a happy and successful adult life, pupils need knowledge that will enable them to make informed decisions about their wellbeing, health and relationships and to build their self-efficacy. Pupils can also put this knowledge into practice as they develop the capacity to make sound decisions when facing risks, challenges and complex contexts. Everyone faces difficult situations in their lives. These subjects can support young people to develop resilience, to know how and when to ask for help, and to know where to access support".

The guidance specifically refers to education for all pupils about online safety both as a discrete topic area but also as an integral part of the planned curriculum, " In this guidance where topics occur equally on and offline they are accommodated in the core content under the most applicable theme with the assumption that teachers will deliver them in a context that reflects that pupils will be negotiating issues and opportunities in these areas on and off line. Where there are topics with exclusively online content or implications this is drawn out explicitly".

The guidance also sets out that, "Effective teaching in these subjects will ensure that core knowledge is broken down into units of manageable size and communicated clearly to pupils, in a carefully sequenced way, within a planned programme or lessons. Teaching will include sufficient well-chosen opportunities and contexts for pupils to practise applying and embedding new knowledge so that it can be used skilfully and confidently in real life situations".

Online safety education will be provided in the following ways:

- A planned online safety programme is provided as part of the PSHE and assembly programme and is regularly revisited in Computing and other lessons across the curriculum – this programme covers both the use of ICT and new technologies in school and outside of school.
- A range of safeguarding issues are considered as part of the online safety education: keeping their personal information private, healthy relationships on and off line, grooming, sending inappropriate images and the consequences of this, gaming, gambling, radicalisation and how to recognise the signs and keep themselves safe
- Pupils are taught in lessons to be critically aware of the materials/content they access on-line and are guided to validate the accuracy of the information.
- Pupils are helped to understand the need for the Pupil AUP and encouraged to adopt safe and responsible use of ICT, the Internet and mobile devices both within and outside of school.
- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the Internet.
- Rules for the use of ICT systems and the Internet are posted in school
- Staff act as good role models in their use of ICT, the Internet and mobile devices.

The government and a range of supporting organisations have produced Education for a Connected World – a Framework to equip children and young people for a digital life (from Early Years upwards) which can be accessed at
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/683895/Education_for_a_connected_world_PDF.PDF

School can access the North Yorkshire curriculum entitlement framework for PSHE and Citizenship which sets out suggested learning outcomes for key stages 1-4 and provides links to supporting age appropriate resources which includes online safety (there are also named resources to teach about grooming, sexting, child sexual exploitation, pornography, radicalisation and extremism which are also safeguarding issues which arise on and off line). The documents can be accessed at http://cyps.northyorks.gov.uk/health-wellbeing-phse

A useful key document to read is the 'Key principles of effective prevention education' - produced by the PSHE Association on behalf of CEOP. These principles will help PSHE education professionals to teach high-quality online safety education as part of their broader PSHE programmes.
https://www.pshe-association.org.uk/curriculum-and-resources/resources/key-principles-effective-prevention-education

Appropriate use of Email

- Digital communications with pupils and parents / carers (e-mail, online chat, VLE, voice etc.) should be on a professional level and only carried out using official school systems
- The federation school's e-mail service should be accessed via the provided web-based interface by default
- Under no circumstances should staff or governors contact pupils, parents/carers or conduct any school business using personal e-mail addresses
- School e-mail is not to be used for personal use
- All staff should be aware that emails can be part of Freedom of Information requests so all correspondence needs to be professional, courteous and respectful
- If confidential information / information under the data protection act is being sent by email it must be sent through the secure email system which if provided by Schools ICT would be the Egress system which the schools administration and headteacher/head of school have access to but more licenses can be purchased.

Appropriate use of mobile phones

- School mobile phones only should be used to contact parents/carers/pupils when on school business with pupils off site. Staff should not use personal mobile devices and under no circumstances should a pupil or parent/carers be given a member of staffs personal mobile number
- Staff should not be using personal mobile phones in school during working hours when in contact with children
- Visitors will be asked not to use their mobile phone whilst on site with any pupils presence due to all mobile phones containing a camera
- Pupils should adhere to the rules and guidelines set out in the Behaviour Policy / mobile phone policy regarding mobile phone use in school

Appropriate use of social networking sites

- Staff should not access social networking sites on school equipment in school or at home that have not been pre-approved by the school
- Staff users and governors should not refer to any member of staff, the governing body, pupils, parents/carers, the school or any other member of the school community on any social networking site or blog in a derogatory way
  - Pupils will not be allowed on social networking sites on school equipment that have not been pre-approved whether in school or at home. At home it is the parental responsibility, but parents should be aware that it is illegal for children under the age of 13 to be on certain social networking sites

- Pupils/Parents/carers should be aware the school will investigate misuse of social networking if it impacts on the well-being of other pupils or members of the school community
- Parents / carers and pupils will be informed that they do not use social media to criticise or make inappropriate comments about the school, an individual member of staff or another pupil as making defamatory comments online has exactly the same legal consequences as if they are made directly to someone else. Similarly threats of violence can lead to criminal proceedings under the Malicious Communications Act. If as a parent/ carer they have any concerns about anything which happens in schools then they will be asked to contact the school directly
- If inappropriate comments are placed on social networking sites about the school or school staff then advice would be sought from the relevant agencies, including the police if necessary
- Pupils will be taught about online safety when using social networking sites

Appropriate use of digital images

- The school record of parental permissions granted/not granted must be adhered to when taking images of our pupils. The list can be obtained from the designated safeguarding lead
- Under no circumstances should images be taken by staff or governors using privately owned equipment
- Permission to use images of all staff and governors who work at the school is sought on induction and a copy is located in the personnel file
- Visitors / contractors will be asked not to use their mobile phone whilst on site with any pupils presence due to all mobile phones containing a camera
- Schools need to decide if parents/ carers can take images from a school event e.g school play, sports day and how those images can be used, as some parents may object to images of their children being on social networking sites. Schools could decide that parents/ carers need to sign an agreement that they will not share photographs taken at school event through any public median or other schools have decided that the school only will take official photographs taken from the event that parent/ carers could then access. This decision needs to be clearly communicated to all parents/ carers and the reasons behind the decision.
- Schools and settings will liaise with external providers and places visited on school trips to ensure they do not take photographs and use the images on their website / social media without permission of a member of staff from the school.

Although many of the above points are preventative and safeguarding measures, it should be noted that the school will endeavour whenever possible to use social networking in positive ways to publicise, inform and communicate information. For example the school may have an active website and Twitter/ Facebook account / blog which are used to inform, publicise school events and celebrate and share the achievement of students.

Removable Data Storage Devices

- Only school provided removable devices should be used and they should be encrypted
- Any information that is on removable data storage device for school use should not be transferred onto any personal devices, in particular any information that is covered by the data protection act and could lead to an individual being identified
- All files downloaded from the Internet, received via e-mail or provided on removable media (e.g. CD, DVD, USB flash drive, memory cards etc.) must be checked for viruses using school provided anti-virus software before run, opened or copied/moved on to local/network hard disks
- Pupils should not bring their own removable data storage devices into school for use on school equipment.

Appropriate use of websites

- 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 will preview any recommended sites before use
- "Open" searches (e.g. "find images/ information on...") are discouraged when working with pupils who may misinterpret information
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by staff. Parents/ carers will be advised to supervise any further research
- All users must observe copyright of materials published on the Internet
- Teachers will carry out a risk assessment regarding which pupils are allowed access to the internet with minimal supervision. Minimal supervision means regular checking of the pupils on the internet by the member of staff setting the task. All staff are aware that if they pass pupils working on the internet that they have a role in checking what is being viewed. Pupils are also aware that all internet use at school is monitored and logged.
- The school only allows the ICT technician and SLT to access to Internet logs.

Passwords are an important element of keeping the users of the schools ICT systems safe

Use of passwords for staff and governors

- Passwords or encryption keys should not be recorded on paper or in an unprotected file
- Passwords should be changed at least every 3 months
- Users should not use the same password on multiple systems or attempt to "synchronise" passwords across systems

Use of passwords for pupils

- Should only let school staff know their in-school passwords
- Should not share their password with another pupil / sibling
- Inform staff immediately if passwords are traced or forgotten. All staff are able to access the network to allow pupils to change passwords

Use of School ICT Equipment

- Privately owned ICT equipment should never be connected to the school's network and no personally owned applications or software packages should be installed on to school ICT equipment
- Personal or sensitive data should not be stored on the local drives of desktop or laptop PCs. If it is necessary to do so, the local drive must be encrypted
- All should ensure any screens are locked before moving away from a computer during the normal working day to protect any personal, sensitive, confidential or classified data and to prevent unauthorised access
- If the school provides ICT equipment for pupils to use at home this needs to be part of the pupil and parent/carer AUP to ensure it is only used for school work and only suitable resources are accessed on the device. The device will be set up to minimise the pupil being able to access any inappropriate information. Parent/ carers will also be asked to set up parental controls on their own broadband provider to try to prevent pupils accessing inappropriate materials and guidance will be provided on how to do this. There will be a specific focus on SEND pupils who are often provided with technology to support their learning.

Monitoring
All use of the federation schools' Internet access is logged and the logs are randomly but regularly monitored by the school's external provider. Schools accessing their internet support from Schools ICT can now access Smoothwall's reporting mechanism which will identify pupils that are searching for websites / using search words that may be inappropriate. It will also highlight issues through the content of the site e.g reference to suicide. This reporting mechanism is all included in the contract with Schools ICT smoothwall so they can provide more information. Other providers are available.

Incident Reporting
Any online safety incidents must immediately be reported to the designated safeguarding lead if it is a member of staff, pupil or parent/carer who will investigate further following online safety and safeguarding policies and guidance.

Responding to incidents of misuse
It is hoped that all members of the school community will be responsible users of ICT. However, there may be times when infringements of the policy could take place through careless or irresponsible, or very rarely, through deliberate misuse. Appendix 1 is a table which provides guidelines on the use of communication technologies. Listed in Appendix 2 are a range of activities that are unacceptable and / or illegal. Appendix 3 and 4 are responses that will be made to any apparent or actual incidents of misuse from pupils and staff. If any apparent or actual, misuse appears to involve illegal activity e.g. child sexual abuse images, adult material which potentially breaches the Obscene Publications Act, criminally racist material or other criminal conduct, activity or materials the tables should be consulted and liaison with the Police should take place. Actions will be followed in accordance with policy, in particular the sections on reporting the incident to the police and the preservation of evidence. If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. It is recommended that more than one member of staff is involved in the investigation. It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with.

When considering an online safety incident involving a pupil(s) a school does need to take into account the nature of the incident, the age of the child and if there is a need to involve any partner agencies. The vulnerability checklist can provide a wider understanding of a range of risk factors that may be impacting on children and young people.
http://www.safeguardingchildren.co.uk/vcl-v3

The Local Safeguarding board has a number of practice guides for professionals which contain information and referral pathways, the aspects that could be highlighted from an online safety incident include such as Extremism and Child Sexual Exploitation. All practice guides can be accessed at http://www.safeguardingchildren.co.uk/professionals/practice-guidance

Sexting in schools and colleges: responding to incidents and safeguarding young people - UKCCIS Guidance
https://www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis
This is clear guidance to schools about how they should handle incidents where pupils under-18 take and/or share naked images of other under-18s, including themselves. This new guidance takes a safeguarding focus, rather than a simple criminal response, and, in some circumstances, allows schools to deal with incidents without involving the police.

There is no clear definition of 'sexting'. Instead, this document talks about 'youth-produced sexual imagery'. This is imagery that is being created by under 18s themselves and involves still photographs, video, and streaming. In the guidance, this content is described as sexual and not indecent.

Incidents covered by this guidance:

- Person under 18 creates a sexual image of themselves and shares it with another person under 18.
- A person under 18s shares an image of another under 18 with another person under 18 or an adult.
- A person under 18 is in possession of sexual imagery created by another person under 18.

Incidents not covered by this guidance:

- Under 18s sharing adult pornography.
- Under 18s sharing sexual texts without sexual imagery.
- Adults sharing sexual imagery of under 18s. (This is child sexual abuse and must always be reported to police.)

The UKCCIS guidance 'Sexting in schools and colleges, responding to incidents and safeguarding young people' published in August 2016, is non-statutory, but should be read alongside 'Keeping children safe in education'. This is important guidance and should be read and understood by DSLs, appropriately communicated to the staff team and incorporated into the schools online safety policy.

Continued……

Appendix 1

The Ryedale Federation's guidelines on the use of communication technologies.

	Staff and other adults				Pupils			
Communication Technologies	Permitted	Permitted at certain times	Permitted for named staff	Not Permitted	Permitted	Permitted at certain times	Allowed with staff permission	Not Permitted
Mobile phones may be brought to school	✓				✓			
Mobile phones used in lessons				✓			✓ e.g taking a photo of some work for revision purposes	
Use of mobile phones in social time	✓					✓ within the mobile phone policy		
Staff should only contact a pupil on a school issued mobile phone	✓							
Taking photographs/film on personal mobile devices / digital camera				✓				✓
Taking photographs/film on school mobile devices / digital camera for school purposes only	✓						✓	
Parent / carer taking photos of a school event on their own device and uploading online with public access				✓				✓
Use of personal tablets/ laptops ipads etc in school				✓				✓
Use of school owned tablets/ laptops/ ipads in school but not for personal use	✓				✓			
Use of school owned tablets/ laptops/ ipads out of school but not for personal use	✓ (within the AUP)				✓ (within the AUP)			

Only using school provided encrypted storage devices		✓					✓			
Use of school email for personal emails					✓					✓
Social use of chat rooms/facilities					✓					✓
Use of social network sites in school				✓					✓	
Use of educational blogs		✓					✓			

When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Staff, governors, volunteers and students should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users need to be aware that email communications may be monitored
- Users must immediately report, to the nominated person (in accordance with the school policy) the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff, governors and pupils or parents/carers (email, chat, Learning Platform etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat/social networking programmes must not be used for these communications.
- Students should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff and governors.

Appendix 2

Unsuitable / inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other ICT systems. Other activities e.g. Cyber- bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities. The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts certain internet usage as follows. Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

User actions	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Child sexual abuse images					✓
Promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation					✓
Adult material that potentially breaches the Obscene Publications Act in the UK					✓
Criminally racist material in the UK					✓
Pornography					✓
Promotion of any kind of discrimination				✓	
Any Hate Crime – motivated by hostility on the grounds of race, religion, sexual orientation, disability or transgender identity.					✓
Promotion of any kind of extremist activity					✓
Promotion of racial or religious hatred					✓
Accessing any extremist materials online (e.g Far Right Extremism)				✓	
Threatening behaviour, including promotion of physical violence or mental harm					✓
Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute e.g discussing school issues on social media				✓	
Using school systems to run a private business				✓	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school				✓	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions				✓	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)				✓	
Creating or propagating computer viruses or other harmful files				✓	
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet				✓	
On-line gaming (educational)		✓			
On-line gaming (non- educational)				✓	
On-line gambling				✓	
On-line shopping / commerce			✓		

File sharing			✓		
Use of social networking sites			✓		
Downloading video broadcasting e.g. Youtube for educational purposes	✓				
Uploading to video broadcast e.g. Youtube			✓		

Continued…..

Appendix 3
Incidents Involving pupils and action taken

Incident involving pupils – either in school or out of school – it could be a concern raised by a friend/ parent	**Teacher to use school behaviour policy to deal with**	**Refer to Pastoral Senior member of staff**	**Record and monitor the pupils behaviour and refer to external agencies if required**	**Refer to technical support staff for action re security/filtering etc**
A concern raised by a pupil/ teacher / friend/ parent (carer). A pupil need positive support – Signs of grooming Signs of peer on peer abuse / grooming / power domination Signs of radicalisation Signs of CSE Signs of cyberbullying		✓	✓	
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/ inappropriate activities**).**		✓	✓	✓
Unauthorised use of non-educational sites during lessons	✓			✓
Unauthorised use of mobile phone/ digital camera/ other handheld device.	✓			
Unauthorised use of social networking/ instant messaging/ personal email and online gaming	✓	✓		✓
Unauthorised downloading or uploading of files		✓		✓
Allowing others to access school network by sharing username and passwords		✓		✓
Attempting to access or accessing the school network, using another student's account		✓		✓
Attempting to access or accessing the school network, using the account of a member of staff		✓		✓
Corrupting or destroying the data of other users		✓		✓
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		✓	✓	✓
Continued infringements of the above, following previous warnings or sanctions		✓	✓	✓
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		✓	✓	✓
Using proxy sites or other means to subvert the school's filtering system		✓	✓	✓
Accidentally accessing offensive or pornographic material and failing to report the incident		✓		✓

Appendix 4
Incidents involving members of staff and action taken

Incidents involving members of staff	**Refer to the Secondary Director/Head of School *See below**	**Refer to technical support staff for action re filtering, security etc**	**Potential Disciplinary Action**
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable /inappropriate activities).	✓	✓	✓
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	✓		✓
Excessive or inappropriate personal use of the internet/social networking sites/ instant messaging/ personal email	✓	✓	✓
Unauthorised downloading or uploading of files	✓	✓	✓
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account.	✓	✓	✓
Careless use of personal data e.g. holding or transferring data in an insecure manner	✓		✓
Deliberate actions to breach data protection or network security rules	✓	✓	✓
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	✓	✓	✓
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	✓	✓	✓
Using personal email/ social networking/ instant messaging/ text messaging to carrying out digital communications with students/ pupils	✓	✓	✓
Actions which could compromise the staff member's / governors professional standing	✓		✓
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	✓		✓
Using proxy sites or other means to subvert the school's filtering system	✓	✓	✓
Deliberately accessing or trying to access offensive or pornographic material	✓	✓	✓
Breaching copyright or licensing regulations	✓	✓	✓
Continued infringements of the above, following previous warnings or sanctions	✓	✓	✓

*In event of breaches of policy by the Secondary Director / Head of School refer to the Chair of Governors.

Appendix 5
Acceptable Internet Use Policy – Pupils

This document is a guide to young people to be responsible and stay safe while using the Internet and other communication technologies. It clearly states what use of computer resources is acceptable and what is not. Irresponsible use may result in the loss of Internet or computer access, contact with parents or in the event of illegal activities contact with the police.

- I will only access the school network through my authorised username and password. I will not use the passwords of others. I will always log off after using the school network.
- I will not use the school IT systems / devices for personal or recreational use, for accessing social media sites, on-line gaming, gambling, internet shopping, file sharing or video broadcasting.
- I will not try to upload, download or access any materials which are illegal, inappropriate or which may cause harm and distress to others.
- I will not try to use any programmes or software that might allow me to bypass the filtering and security systems in place.
- I will not try to install programmes on any school computer or try to alter computer settings.
- I will only use my personal electronic devices (e.g. mobile phone/ipod) in school at times that are permitted; travelling to and from school, contacting parents after participation in an extra-curricular activity, or when permitted to do so by a member of staff. When using my own devices I understand that I have to follow the rules set out in this document.
- I will carefully write email and other on-line messages making sure the language I use is not strong, aggressive or inappropriate and shows respect for others. I am responsible for the emails I send and the contacts I make.
- I will not open emails unless I know and trust the person/organisation who has sent them.
- For my own safety and that of others, I will not disclose personal information about myself or others when on-line. I will not arrange to meet someone I do not know.
- I will not take, or distribute, images of anyone else without their permission.
- I will not take, or distribute, images of myself or anyone else semi-naked or naked.
- I will only use chat and social networking sites with permission and at the times that are allowed.
- I will report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.
- Where the material I research on the Internet is protected by copyright, I will not try to download copies, including music and video. I will only use the work of others found on the Internet in my own work with their permission.
- I will take care to check that information I find on the Internet is accurate and understand that some work found on the Internet can be untruthful or misleading.
- I will immediately report any damage or faults involving IT equipment, however this may have happened.
- I will not bring the school into disrepute by making inappropriate comments on social media.

Please note that the school may exercise its right to monitor the use of the computer system, including monitoring access to websites, the interception of emails and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system is or may be taking place , or the system is or may be being used for criminal purposes or for storing unlawful text, imagery or sound.

Student Signature: …….. Date: ……..

Parent/Carer Signature: …….. Date …….

Appendix 6
Acceptable Internet Use Policy – Adults who work in the school community
(this includes governors and volunteers)

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The Internet and other digital information and communications are powerful tools, which open up new opportunities for everyone. These technologies can inspire discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users have an entitlement to safe Internet access at all times.

This policy is intended to ensure that:

- Staff, governors and volunteers will be responsible users and stay safe while using the Internet and other communications technologies for educational, personal and recreational use.
- All school ICT systems users are protected from accidental or deliberate misuse that could put the security of the systems or users at risk.
- Staff are protected from potential risk in their use of ICT in their everyday work.

The federation schools will try to ensure that staff, governors and volunteers will have good access to ICT to enhance their work, to improve learning opportunities for all and will, in return, expect staff, governors and volunteers to agree to be responsible users.

Responsible Use Agreement

I understand that I must use the school's ICT systems in a responsible way to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that learners receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with students.

For my professional and personal safety:

- I understand that the school will monitor my use of ICT systems, email and other digital communications.
- I understand the rules set out in this agreement also apply to the use of the school ICT systems (e.g. laptops, email, Learning Platform etc.) out of the school.
- I will only use school ICT equipment for school purposes. I will not use any personal devices for any school business unless accessing a secure online platform specifically provided by the school
- I will not store any school data (in line with the schools data protection policy) on personal devices
- I understand that the school ICT systems are intended for educational use and that I will not use systems for personal or recreational use.
- I will not disclose my username and password to anyone else, nor will I try to use any other person's username and password.
- I will immediately report any illegal, inappropriate or harmful material/incident I become aware of to the appropriate person.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files without their express permission.
- I will communicate with others in a professional manner. I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I am aware that emails can be part of Freedom of Information requests so all my correspondence will be professional, courteous and respectful
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images. I will not use my personal equipment to record these images.
- I will not use chat and social networking sites in the school in accordance with the school's policies.
- I will only communicate with student and parents/carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.
- I will not befriend any present pupil on social media
- *For Governors I will not add new families as social media contacts whilst a governor*
- I will not 'discuss' any school issues on social media. *For governors this is covered in the Governors code of conduct*
- I will not use personal email addresses on the school ICT systems.
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will ensure that my data is regularly backed up, in accordance with relevant policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not (unless I have permission) make large downloads or uploads that might take up Internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport and hold data about others that is protected by the Data Protection Act in an encrypted manner. I will not transfer any data to any personal devices.
- I understand that data protection policy requires that any staff, governor or learner data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

Internet Use

The School provides internet access to employees to assist with performance of their duties.

Personal Use

Whilst the internet should primarily be used for business functions, incidental and occasional use of the internet in a personal capacity may be permitted so long as:

- Usage does not tarnish the reputation of the School,
- Employees understand that School management may have access to their internet browsers and

browsing history contained within,
- Employees understand that the School reserves the right to suspend internet access at any time,
- Use of the internet for personal use does not infringe on business functions.

Inappropriate Use

The School does not permit individuals use the internet in a way that may be interpreted as insulting, disruptive, or offensive by any other individual or entity. Examples of prohibited material include, but are not necessarily limited to:

- Sexually explicit or pornographic images, cartoons, jokes or movie files,
- Images, cartoons, jokes or movie files containing ethnic, religious, or racial slurs,
- Any content that could be construed as harassment or disparagement of others based on their sex, gender, racial or ethnic origin, sexual orientation, age, disability, religious or philosophical beliefs, or political beliefs.

Individuals are also not permitted to use the internet in a way which could affect usage for others. This means not streaming or downloading media files and not using the internet for playing online games.

Other Business Use

Users are not permitted to use the internet to carry out their own business or business of others. This includes, but not necessarily limited to, work for political organisations, not-for-profit organisations, and private enterprises. This restriction may be lifted on a case by case basis at the discretion of School management.

I understand that I am responsible for my actions in and out of the school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of the school.

- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and, in the event of illegal activities, the involvement of the police.

I have read and understand the above and agree to use the school ICT systems (both in and out of school) within these guidelines.

<u>Staff/Volunteer/ Governor</u>

Name (please print): ……..

Signature: ……..

Date: ……

Appendix 7

Home - School agreement OR Acceptable Internet Use Policy Parents / Carers

The following could be include in a home – school agreement form that many schools already have in place

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The Internet and other digital information and communications are powerful tools, which open up new opportunities for everyone. These technologies can inspire discussion, promote creativity and stimulate awareness of context to promote effective learning. However, the use of these new technologies can put young people at risk within and outside the school. All users have an entitlement to safe Internet access at all times.

To support parents / carers in learning about the online risks, support you to be able to talk to your children the risks and learn how to set up parental controls there is a section on our school website signposting you to range of supporting websites.

As a parent / carer of a child at a Ryedale Federation School we are asking that you:

- Will contact school and all members of staff within school through the appropriate school communication channels and treat everyone with respect and professionalism. You will not contact any member of staff through a personal email address or phone number
- Ensure you do not use social media to criticise or make inappropriate comments about the school or an individual member of staff as making defamatory comments online has exactly the same legal consequences as if they are made directly to someone else. Similarly threats of violence can lead to criminal proceedings under the Malicious Communications Act. If as a parent/ carer you have any concerns about anything which happens in schools then please contact the school directly
- Ensure that any school technology that is brought home by your child is used appropriately for school based work and that where available your home internet provider will have parental controls set that minimise the risk of your child accessing anything inappropriate online
- Ensuring that school equipment is only used by the pupil who the equipment has been provided for and no other family member, sibling or friends use the equipment
- Ensure that you have signed the Consent Preferences form which sets out that *any photographs/films that are taken of school events may not be shared on any publically accessed social networking site or website, without explicit permission by the Secondary Director/Head of School.*