Scholes (Elmet) Primary | St James' CE Primary | Moortown Primary

Online Safety policy

Adopted: May 2020 **Next review:** annually, unless any changes are required prior to this
Reviewed: November 2021

Introduction

Key people / dates

Sphere Federation	Designated Safeguarding Lead (DSL) team	**Senior safeguarding lead across Sphere Federation:** Clare Weekes **Moortown:** Clare Weekes **Scholes:** Karen Hague **St James':** Natalie Beatson
	Online-safety lead (if different)	Paul Wilks
	Online-safety / safeguarding link governor	Rachel Greenhalgh
	Living and Learning (PSHE/RSHE lead)	Caroline Taylor, Vicky Latham
	Network manager / other technical support	AdEPT
	Date this policy was reviewed and by whom	November 2021, Paul Wilks
	Date of next review and by whom	November 2021, Paul Wilks

What is this policy?

This policy was written as a model policy for a particular school but in this document includes all schools in Sphere Federation.

Online safety is an integral part of safeguarding and requires a whole school, cross-curricular approach and collaboration between key school leads. Accordingly, this policy is written in line with 'Keeping Children Safe in Education' (KCSIE), 'Teaching Online Safety in Schools' and other statutory documents. It complements existing and forthcoming subjects including Computing, Living and Learning (Health, Relationships and Sex Education, Citizenship) and any other relevant subject. It is designed to sit alongside the school's statutory Safeguarding Policy.

Any issues and concerns with online safety must follow the school's safeguarding and child protection procedures.

Who is it for; when is it reviewed?

This policy is a living document, subject to full annual review but also amended where necessary during the year in response to developments in the school and local area. Although many aspects will be informed by legislation and regulations, we involve staff, governors, pupils and parents in writing and reviewing the policy (KCSIE stresses making use of teachers' day-to-day experience on the ground). This will help ensure all stakeholders understand the rules that are in place and why, and that the policy affects day-to-day practice. Acceptable Use Policies (see appendices) for different stakeholders help with this – these are reviewed alongside this overarching policy. Any changes to this policy are immediately disseminated to all stakeholders.

Who is in charge of online safety?

There is a named online-safety coordinator at each school (see above); this person is also the designated safeguarding lead (DSL). KCSIE makes clear that "the designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety)."

What are the main online safety risks today?

Online-safety risks are traditionally categorised as one of the 4 Cs: Content, Contact, Conduct and Commerce (identified by Professor Tanya Byron's 2008 report "Safer children in a digital world"). These four areas remain a helpful way to understand the risks and potential school response, whether technological or educational. They do not stand in isolation, however, and it is important to understand the interplay between all four. Many of these new risks are mentioned in KCSIE, e.g. fake news, upskirting and password phishing.

A 2018 pupil survey (LGFL, DigiSafe) of 40,000 pupils identified an increase in distress caused by, and risk from, content. For many years, online-safety messages have focussed on 'stranger danger', ie meeting strangers online and then meeting them face to face (contact). Whilst these dangers have not gone away and remain important, other online risks such as the sharing of violent or sexual content, persuasive techniques to gain personal data or coerce individuals into dangerous actions are prevalent.

How will this policy be communicated?

This policy can only impact upon practice if it is a (regularly updated) living document. It must be accessible to and understood by all stakeholders. It will be communicated in the following ways:

- Posted on the school website
- Available in paper format in the school
- Part of school induction pack for all new staff (including temporary, supply and non-classroom-based staff)
- Integral to safeguarding updates and training for all staff (especially in September refreshers)
- Clearly reflected in the Acceptable Use Policies (AUPs) for staff, volunteers, governors, external groups, pupils and parents/carers.

- AUPs will be thoroughly reviewed with pupils who will agree to follow it by signing every year.
- AUPs are displayed in appropriate classrooms.
- Reviews of this online-safety policy will include input from staff, pupils and other stakeholders, helping to ensure further engagement

Contents

Overview

Aims

This policy aims to:

- Set out expectations for all Sphere Federation community members' online behaviour, attitudes and activities and use of digital technology (including when devices are offline)
- Help all stakeholders to recognise that online/digital behaviour standards (including social media activity) must be upheld beyond the confines of the school gates and school day, and regardless of device or platform
- Facilitate the safe, responsible and respectful use of technology to support teaching & learning, increase attainment and prepare children and young people for the risks and opportunities of today's and tomorrow's digital world, to survive and thrive online
- Help school staff working with children to understand their roles and responsibilities to work safely and responsibly with technology and the online world:
    - for the protection and benefit of the children and young people in their care, and
    - for their own protection, minimising misplaced or malicious allegations and to better understand their own standards and practice
    - for the benefit of the school, supporting the school ethos, aims and objectives, and protecting the reputation of the school and profession
- Establish clear structures by which online misdemeanours will be treated, and procedures to follow where there are doubts or concerns (with reference to other school policies such as the Positive Relationships Policy)

Further Help and Support

Internal school channels should always be followed first for reporting and support, as documented in school policy documents, especially in response to incidents, which should be reported in line with the Safeguarding Policy. The DSL will handle referrals to the local authority and normally the Head of School / Head of Federation will handle referrals to the LA designated officer (LADO). The local authority or third-party support organisations we work with may also have advisors to offer general support.

Beyond this, **reporting.lgfl.net** has a list of curated links to external support and helplines for both pupils and staff, including the Professionals' Online-Safety Helpline from the UK Safer Internet Centre and the NSPCC Whistleblowing Helpline, as well as hotlines for hate crime, terrorism and fraud which might be useful to share with parents, and anonymous support for children and young people.

Scope

This policy applies to all members of the Sphere Federation community (including staff, governors, volunteers, contractors, students/pupils, parents/carers, visitors and community users) who have access to our digital technology, networks and systems, whether on-site or remotely, and at any time, or who use technology in their school role.

Roles and responsibilities

This federation is a community and all members have a duty to behave respectfully online and offline; to use technology for teaching and learning and to prepare for life after school; and to immediately report any concerns or inappropriate behaviour to protect staff, pupils, families and the reputation of the school. We learn together, make honest mistakes together and support each other in a world that is online and offline at the same time.

Head of Federation – David Roundtree

Key responsibilities:

- Foster a culture of safeguarding where online safety is fully integrated into whole-school safeguarding
- Oversee the activities of the designated safeguarding leads and ensure that the DSL responsibilities listed in the section below are being followed and fully supported
- Ensure that policies and procedures are followed by all staff
- Undertake training in offline and online safeguarding, in accordance with statutory guidance and Leeds Safeguarding Children's Partnership (LSCP)
- Liaise with the designated safeguarding leads on all online-safety issues which might arise and receive regular updates on school issues and broader policy and practice information
- Take overall responsibility for data management and information security ensuring the school's provision follows best practice in information handling; work with the DPO, DSL and governors to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Ensure the school implements and makes effective use of appropriate ICT systems and services including school-safe filtering and monitoring, protected email systems and that all technology including cloud systems are implemented according to child-safety first principles
- Be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles
- Understand and make all staff aware of procedures to be followed in the event of a serious online safeguarding incident
- Ensure suitable risk assessments are undertaken so the curriculum meets needs of pupils, including risk of children being radicalised
- Ensure that there is a system in place to monitor and support staff (e.g. network manager) who carry out internal technical online-safety procedures
- Ensure governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety
- Ensure the school website meets statutory requirements

Designated Safeguarding Lead: Clare Weekes (Moortown), Karen Hague (Scholes), Natalie Beatson (St James') working closely with the Online Safety Lead: Paul Wilks

Key responsibilities (remember the DSL can delegate certain online-safety duties, e.g. to the online-safety coordinator, but not the overall responsibility; this assertion is from Keeping Children Safe in Education):

- "The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety)."
- Ensure "An effective approach to online safety [that] empowers a school or college to protect and educate the whole school or college community in their use of technology and establishes mechanisms to identify, intervene in and escalate any incident where appropriate."
- "Liaise with the local authority and work with other agencies in line with Working together to safeguard children"
- Take day to day responsibility for online safety issues and be aware of the potential for serious child protection concerns
- Work with the Head of Federation, DPO and governors to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Stay up to date with the latest trends in online safety
- Review and update this policy, other online safety documents (eg Acceptable Use Policies) and the strategy on which they are based (in harmony with policies for behaviour, safeguarding, Prevent and others) and submit for review to the governors
- Receive regular updates in online safety issues and legislation, be aware of local and school trends – see safeblog.lgfl.net for examples or sign up to the LGfL safeguarding newsletter
- Ensure that online safety education is embedded across the curriculum (eg by use of the UKCIS framework 'Education for a Connected World') and beyond, in wider school life
- Promote an awareness and commitment to online safety throughout the school community, with a strong focus on parents, who are often appreciative of school support in this area, but also including hard-to-reach parents
- Liaise with school technical, pastoral, and support staff as appropriate
- Communicate regularly with SLT and the designated safeguarding and online safety governor to discuss current issues (anonymised), review incident logs and filtering control logs
- Ensure all staff are aware of the procedures that need to be followed in the event of an online safety incident, and that these are logged in the same way as any other safeguarding incident
- Oversee and discuss 'appropriate filtering and monitoring' with governors (is it physical or technical?) and ensure staff are aware (Ofsted inspectors have asked classroom teachers about this).
- Ensure the 2021 DfE guidance on sexual violence and harassment is followed throughout the school and that staff adopt a zero-tolerance approach to this, as well as to bullying
- Facilitate training and advice for all staff:

- all staff must read KCSIE Part 1 and all those working with children Annex A
- it would also be advisable for all staff to be aware of Annex C (online safety)
- cascade knowledge of risks and opportunities throughout the organisation
- cpd.lgfl.net has helpful CPD materials including PowerPoints, videos and more

Governing Body, led by Online Safety / Safeguarding Link Governor – Rachel Greenhalgh

Key responsibilities (Keeping Children Safe in Education):

- Approve this policy and strategy and subsequently review its effectiveness, eg by asking the questions in the helpful document from the UK Council for Child Internet Safety (UKCIS) Online safety in schools and colleges: Questions from the Governing Board
- "Ensure an appropriate **senior member** of staff, from the school or college leadership team, is appointed to the role of DSL [with] **lead responsibility** for safeguarding and child protection (including online safety) [with] the appropriate status and authority [and] time, funding, training, resources and support…"
- Support the school in encouraging parents and the wider community to become engaged in online safety activities
- Have regular strategic reviews with the online-safety co-ordinator / DSL and incorporate online safety into standing discussions of safeguarding at governor meetings
- Work with the DPO, DSL and Head of Federation to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Check all school staff have read Part 1 of KCSIE; SLT and all working directly with children have read Annex A; check that Annex C on Online Safety reflects practice in your school
- "Ensure that all staff undergo safeguarding and child protection training (including online safety) at induction. The training should be regularly updated […] in line with advice from the local three safeguarding partners […] integrated, aligned and considered as part of the overarching safeguarding approach." There is further support for this at cpd.lgfl.net
- "Ensure appropriate filters and appropriate monitoring systems are in place [but…] be careful that 'overblocking' does not lead to unreasonable restrictions as to what children can be taught with regard to online teaching and safeguarding"
- "Ensure that children are taught about safeguarding, including online safety […] as part of providing a broad and balanced curriculum […] Consider a whole school or college approach to online safety [with] a clear policy on the use of mobile technology." NB – you may wish to refer to 'Teaching Online Safety in Schools 2019' and investigate/adopt the UKCIS cross-curricular framework 'Education for a Connected World' to support a whole-school approach

All staff

Key responsibilities:

- Follow this policy, with particular attention to the Acceptable Use Policy (AUP), one of a series of Safeguarding Essentials (there is an expectation that the AUP and Safeguarding Essentials are signed for and followed closely)
- Understand that online safety is a core part of safeguarding; as such it is part of everyone's job – never think that someone else will pick it up
- Know who the Designated Safeguarding Lead (DSL) and Online Safety Lead (OSL) are.
- Read Part 1, Annex A and Annex C of Keeping Children Safe in Education (whilst Part 1 is statutory for all staff, Annex A for SLT and those working directly with children, it is good practice for all staff to read all three sections).
- Read and follow this policy in conjunction with the school's main safeguarding policy
- Record online-safety incidents in the same way as any safeguarding incident and report in accordance with school procedures.
- Understand that safeguarding is often referred to as a jigsaw puzzle – you may have discovered the missing piece so do not keep anything to yourself
- Notify the DSL/OSL if policy does not reflect practice in your school and follow escalation procedures if concerns are not promptly acted upon
- Identify opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum, supporting curriculum leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for pupils)
- Whenever overseeing the use of technology (devices, the internet, new technology such as augmented reality, etc) in school or setting as homework tasks, encourage sensible use, monitor what pupils are doing and consider potential dangers and the age appropriateness of websites (ask your DSL what appropriate filtering and monitoring policies are in place)
- To carefully supervise and guide pupils when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant), supporting them with search skills, critical thinking (e.g. fake news), age appropriate materials and signposting, and legal issues such as copyright and data law
- Prepare and check all online source and resources before using within the classroom
- Encourage pupils to follow their acceptable use policy, remind them about it and enforce school sanctions
- Notify the DSL/OSL of new trends and issues before they become a problem
- Take a zero-tolerance approach to bullying and low-level sexual harassment
- Be aware that you are often most likely to see or overhear online-safety issues (particularly relating to bullying and sexual harassment and violence) in the playground, corridors, toilets and other communal areas outside the classroom – let the DSL/OSL know
- Receive regular updates from the DSL/OSL and have a healthy curiosity for online safety issues – you may find it useful to read at least the headline statistics and conclusions from the LGfL DigiSafe pupil survey of 40,000 pupils (new themes include 'self-harm bullying' and getting undressed on camera)

- Model safe, responsible and professional behaviours in their own use of technology. This includes outside the school hours and site, and on social media, in all aspects upholding the reputation of the school and of the professional reputation of all staff. More guidance on this point can be found in this Online Reputation guidance for schools.

Living and Learning – Caroline Taylor, Vicky Latham

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Embed consent, mental wellbeing, healthy relationships and staying safe online into the Living and Learning (PSHE / Relationships education, relationships and sex education (RSE) and health education) curriculum. "This will include being taught what positive, healthy and respectful online relationships look like, the effects of their online actions on others and knowing how to recognise and display respectful behaviour online. Throughout these subjects, teachers will address online safety and appropriate behaviour in an age appropriate way that is relevant to their pupils' lives."
- This will complement the computing curriculum, which covers the principles of online safety at all key stages, with progression in the content to reflect the different and escalating risks that pupils face. This includes how to use technology safely, responsibly, respectfully and securely, and where to go for help and support when they have concerns about content or contact on the internet or other online technologies.
- Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within PSHE / RSHE.

Curriculum (including Computing) lead – Paul Wilks

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Oversee the delivery of the online safety element of the Computing curriculum in accordance with the national curriculum
- Look for opportunities to embed online safety across the curriculum and model positive attitudes and approaches to staff and pupils alike
- Ensure action plans have an online-safety element
- Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing
- Collaborate with technical staff and others responsible for ICT use in school to ensure a common and consistent approach, in line with acceptable-use agreements

Network Manager/technician – AdEPT

Key responsibilities:

- As listed in the 'all staff' section, plus:

- Keep up to date with the school's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- Work closely with the designated safeguarding lead / online safety lead / data protection officer to ensure that school systems and networks reflect school policy
- Ensure the above stakeholders understand the consequences of existing services and of any changes to these systems (especially in terms of access to personal and sensitive records / data and to systems such as YouTube mode, web filtering settings, sharing permissions for files on cloud platforms etc
- Support and advise on the implementation of 'appropriate filtering and monitoring' as decided by the DSL and senior leadership team
- Maintain up-to-date documentation of the school's online security and technical procedures
- To report online-safety related issues that come to their attention in line with school policy
- Manage the school's systems, networks and devices, according to a strict password policy, with systems in place for detection of misuse and malicious attack, with adequate protection, encryption and backup for data, including disaster recovery plans, and auditable access controls
- Monitor the use of school technology and that any misuse/attempted misuse is identified and reported in line with school policy

Data Protection Officer (DPO) – Carr Manor Support Services

Key responsibilities:

- NB – this document is not for general data-protection guidance
- Be aware that references to the relationship between data protection and safeguarding in key Department for Education documents 'Keeping Children Safe in Education' and 'Data protection: a toolkit for schools' (August 2018), especially this quote from the latter document:
  "GDPR does not prevent, or limit, the sharing of information for the purposes of keeping children safe. Lawful and secure information sharing between schools, Children's Social Care, and other local agencies, is essential for keeping children safe and ensuring they get the support they need. **The Data Protection Act 2018 introduced 'safeguarding' as a reason to be able to process sensitive, personal information, even without consent** (DPA, Part 2,18; Schedule 8, 4) When Designated Safeguarding Leads in schools are considering whether, or not, to share safeguarding information (especially with other agencies) it is considered best practice for them to record who they are sharing that information with and for what reason. If they have taken a decision not to seek consent from the data subject and/or parent/carer that should also be recorded within the safeguarding file. All relevant information can be shared without consent if to gain consent would place a child at risk. Fears about sharing information **must not be allowed** to stand in the way of promoting the welfare and protecting the safety of children."

- The same document states that the retention schedule for safeguarding records may be required to be set as 'Very long term need (until pupil is aged 25 or older)'. However, some local authorities require record retention until 25 for all pupil records.

- Work with the DSL, Head of Federation and governors to ensure frameworks are in place for the protection of data and of safeguarding information sharing as outlined above.
- Ensure that all access to safeguarding data is limited as appropriate, and also monitored and audited

Pupils

Key responsibilities:

- Read, understand, sign and adhere to the pupil Acceptable Use Policy (AUP) and do this annually. If children refuse to sign the AUP, a discussion with parents/carers will be arranged to talk about their refusal which, if still unresolved, will likely result in restricted access to technology in school for the child.
- Understand the importance of reporting abuse, misuse or access to inappropriate materials.
- Know what action to take if they or someone they know feels worried or vulnerable when using online technology.
- To understand the importance of adopting safe and responsible behaviours and good online safety practice when using digital technologies outside of school and realise that the school's acceptable use policies cover actions out of school, including on social media
- Understand the benefits/opportunities and risks/dangers of the online world and know who to talk to at school or outside school if there are problems

Parents/carers

Key responsibilities:

- Read and promote the school's parental Acceptable Use Policy (AUP) and read the pupil AUP and help their children to follow it
- Alert the school if they have any concerns about their children's and others' use of technology
- Promote positive online safety and model safe, responsible and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers.

Volunteers and External groups

Key responsibilities:

- Any external individual/organisation will follow the acceptable use policy prior to using technology or the internet within school
- Support the school in promoting online safety and data protection

- Model safe, responsible, respectful and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers

Education and curriculum

Living and Learning (PSHE, RSE, Health, Citizenship) and Computing have the clearest online safety links (see the relevant role descriptors above for more information):

However, as stated in the role descriptors above, it is the role of all staff to identify opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for pupils)

Whenever overseeing the use of technology (devices, the internet, new technology such as augmented reality, etc) in school or setting as homework tasks, all staff should encourage sensible use, monitor what pupils/students are doing and consider potential dangers and the age appropriateness of websites (ask your DSL/OSL what appropriate filtering and monitoring policies are in place).

Equally, all staff should carefully supervise and guide pupils when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant), supporting them with search skills, critical thinking (e.g. fake news), age appropriate materials and signposting, and legal issues such as copyright and data law.

In Sphere Federation, we recognise that online safety and broader digital literacy must be thread throughout the curriculum. Our Computing and Living & Learning AREs promote this.

Various monitoring and evaluating activities help to ensure online safeguarding.

Handling online-safety concerns and incidents

It is vital that all staff recognise that online-safety is a part of safeguarding as well as being a curriculum strand.

General concerns must be handled in the same way as any other safeguarding concern; safeguarding is often referred to as a jigsaw puzzle, so all stakeholders should err on the side of talking to the designated safeguarding lead to contribute to the overall picture or highlight what might not yet be a problem.

Support staff will often have a unique insight and opportunity to find out about issues first in the playground, corridors, toilets and other communal areas outside the classroom (particularly relating to bullying and sexual harassment and violence).

School procedures for dealing with online-safety will be mostly detailed in the following policies (primarily in the first key document):

- Safeguarding and Child Protection Policy (including Prevent)
- Positive Relationships Policy
- Acceptable Use Policies
- Data Protection Policy, agreements and other documentation (e.g. privacy statement and consent forms for data sharing, image use etc)

This school commits to take all reasonable precautions to ensure online safety, but recognises that incidents will occur both inside school and outside school (and that those from outside school will continue to impact on pupils when they come into school). All members of the school are encouraged to report issues swiftly to allow them to be dealt with quickly and sensitively through the school's escalation processes.

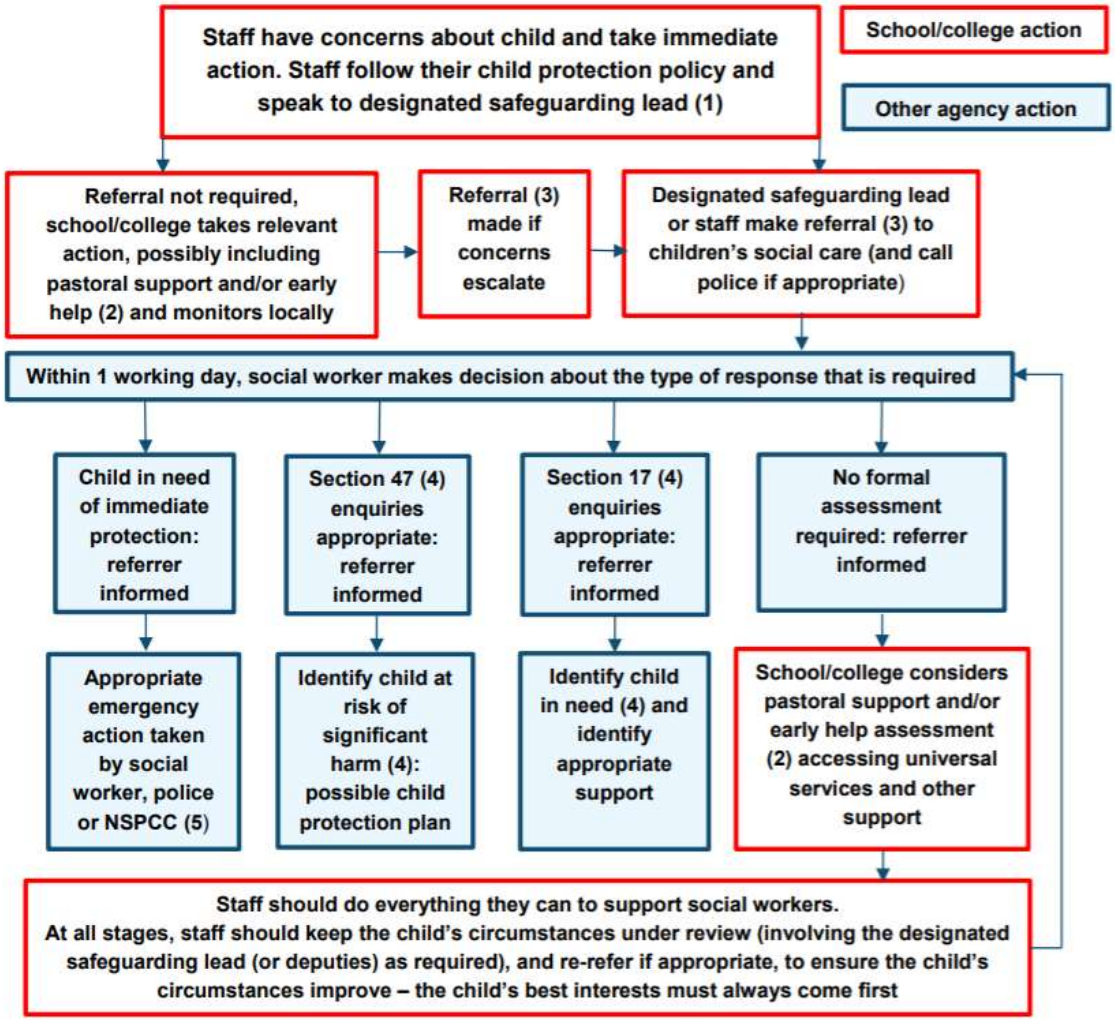
Any suspected online risk or infringement should be reported to the designated safeguarding lead on the same day – where clearly urgent, it will be made by the end of the lesson.

Any concern/allegation about staff misuse is always referred directly to the Head of School / Head of Federation, unless the concern is about the Head of Federation, in which case the complaint is referred to the Chair of Governors and the LADO (Local Authority's Designated Officer). Staff may also use the NSPCC Whistleblowing Helpline.

The school will actively seek support from other agencies as needed (i.e. the local authority, UK Safer Internet Centre's Professionals' Online Safety Helpline, NCA CEOP, Prevent Officer, Police, Internet Watch Foundation). We will inform parents/carers of online-safety incidents involving their children, and the Police where staff or pupils engage in or are subject to behaviour which we consider is particularly disturbing or breaks the law (particular procedures are in place for sexting and upskirting; see section below).

Actions where there are concerns about a child

The following flow chart (it cannot be edited) is taken from Keeping Children Safe in Education as the key education safeguarding document. As outlined previously, online safety concerns are no different to any other safeguarding concern.



(1) In cases which also involve a concern or an allegation of abuse against a staff member, see Part Four of this guidance.

(2) Early help means providing support as soon as a problem emerges at any point in a child's life. Where a child would benefit from co-ordinated early help, an early help inter-agency assessment should be arranged. Chapter one of Working Together to Safeguard Children provides detailed guidance on the early help process.

(3) Referrals should follow the process set out in the local threshold document and local protocol for assessment. Chapter one of Working Together to Safeguard Children.

(4) Under the Children Act 1989, local authorities are required to provide services for children in need for the purposes of safeguarding and promoting their welfare. Children in need may be assessed under section 17 of the Children Act 1989. Under section 47 of the Children Act 1989, where a local authority has reasonable cause to suspect that a child is suffering or likely to suffer significant harm, it has a duty to make enquiries to decide whether to take action to safeguard or promote the child's welfare. Full details are in Chapter one of Working Together to Safeguard Children.

(5) This could include applying for an Emergency Protection Order (EPO).

Sexting

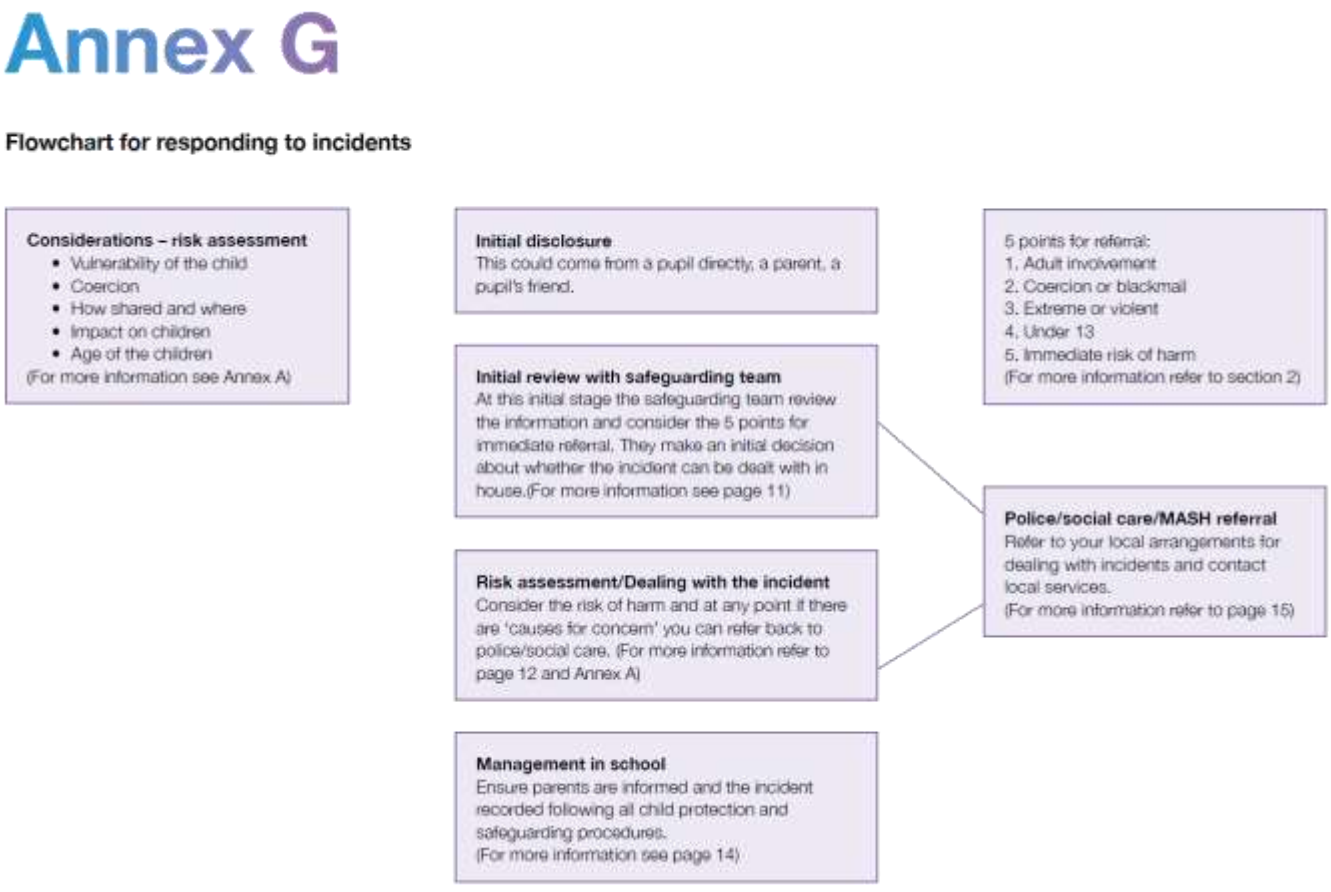
All schools (regardless of phase) should refer to the UK Council for Internet Safety (UKCIS) guidance on sexting (also referred to as 'youth produced sexual imagery') in schools. NB - where one of the parties is over 18, this is no longer sexting but child sexual abuse.

There is a one-page overview called Sexting; how to respond to an incident for all staff (not just classroom-based staff) to read, in recognition of the fact that it is mostly someone other than the designated safeguarding lead (DSL) or online safety lead to first become aware of an incident, and it is vital that the correct steps are taken. Staff other than the DSL must not attempt to view, share or delete the image or ask anyone else to do so, but to go straight to the DSL.

The school DSL will in turn use the full guidance document, Sexting in Schools and Colleges to decide next steps and whether other agencies need to be involved.

It is important that everyone understands that whilst sexting is illegal, pupils/students can come and talk to members of staff if they have made a mistake or had a problem in this area.

The documents referenced above and materials to support teaching about sexting can be found at sexting.lgfl.net



Upskirting

It is important that everyone understands that upskirting (taking a photo of someone under their clothing) is now a criminal offence, as highlighted in Keeping Children Safe in Education and that pupils/students can come and talk to members of staff if they have made a mistake or had a problem in this area.

Bullying

Online bullying should be treated like any other form of bullying and the school's Positive Relationships policy should be followed for online bullying, which may also be referred to as cyberbullying.

Materials to support teaching about bullying and useful Department for Education guidance and case studies are at bullying.lgfl.net

Sexual violence and harassment

DfE guidance on sexual violence and harassment is referenced in Keeping Children Safe in Education and also a document in its own right. It would be useful for all staff to be aware of this guidance: paragraphs 55-61 cover the immediate response to a report and confidentiality which is highly relevant for all staff; the case studies section provides a helpful overview of some of the issues which may arise.

Any incident of sexual harassment or violence (online or offline) should be reported to the DSL who will follow the full guidance. Staff should work to foster a zero-tolerance culture. The guidance stresses that schools must take all forms of sexual violence and harassment seriously, explaining how it exists on a continuum and that behaviours incorrectly viewed as 'low level' are treated seriously and not allowed to perpetuate. The document makes specific reference to behaviours such as bra-strap flicking and the careless use of language.

Misuse of school technology (devices, systems, networks or platforms)

Clear and well communicated rules and procedures are essential to govern pupil and adult use of school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).

These are defined in the relevant Acceptable Use Policy as well as in this document, for example in the sections relating to the professional and personal use of school platforms/networks/clouds, devices and other technology.

Where pupils contravene these rules, the Positive Relationships policy will be applied; where staff contravene these rules, action will be taken as outlined in the staff handbook.

Further to these steps, the school reserves the right to withdraw – temporarily or permanently – any or all access to such technology, or the right to bring devices onto school property.

Social media incidents

See the social media section later in this document for rules and expectations of behaviour for children and adults in the school community. These are also governed by school Acceptable Use Policies.

Breaches will be dealt with in line with the Positive Relationships policy (for pupils) or staff handbook (for staff).

Further to this, where an incident relates to an inappropriate, upsetting, violent or abusive social media post by a member of the school community, the school will request that the post be deleted and will expect this to be actioned promptly.

Where an offending post has been made by a third party, the school may report it to the platform it is hosted on, and may contact the Professionals' Online Safety Helpline (run by the UK Safer Internet Centre) for support or help to accelerate this process.

Data protection and data security

There are references to the relationship between data protection and safeguarding in key Department for Education documents 'Keeping Children Safe in Education' and 'Data protection: a toolkit for schools' (August 2018), which the DPO and DSL will seek to apply.

"**GDPR does not prevent, or limit, the sharing of information for the purposes of keeping children safe.** Lawful and secure information sharing between schools, Children's Social Care, and other local agencies, is essential for keeping children safe and ensuring they get the support they need. **The Data Protection Act 2018 introduced 'safeguarding' as a reason to be able to process sensitive, personal information, even without consent** (DPA, Part 2,18; Schedule 8, 4). When Designated Safeguarding Leads in schools are considering whether, or not, to share safeguarding information (especially with other agencies) **it is considered best practice for them to record who they are sharing that information with and for what reason. If they have taken a decision not to seek consent from the data subject and/or parent/carer that should also be recorded within the safeguarding file. All relevant information can be shared without consent if to gain consent would place a child at risk. Fears about sharing information must not be allowed to stand in the way of promoting the welfare and protecting the safety of children**."

All pupils, staff, governors, volunteers, contractors and parents are bound by the school's data protection policy and agreements. This school makes use of Carr Manor Support Services for GDPR compliance.

Rigorous controls on the school network, USO sign-on for technical services, firewalls and filtering all support data protection. The following data security products are also used to protect the integrity of data, which in turn supports data protection: SonicWall, Impero, Sophos Anti-Virus, Sophos InterceptX, Sophos for Servers, EFT, DFE Sign-in, Synergy Gateway.

The Head of Federation, DPO and governors work together to ensure a GDPR-compliant framework for storing data, but which ensures that child protection is always put first and data-protection processes support careful and legal sharing of information.

Staff are reminded that all safeguarding data is highly sensitive and should be treated with the strictest confidentiality at all times, and only shared via approved channels to colleagues or agencies with appropriate permissions. The use of EFT encrypted file transfer is used to encrypt data. All non-internal emails are password protected and encrypted when containing sensitive information. If this is not possible, the DPO and DSL should be informed in advance.

Appropriate filtering and monitoring

Keeping Children Safe in Education obliges schools to "ensure appropriate filters and appropriate monitoring systems are in place [and] not be able to access harmful or inappropriate material [but at the same time] be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding."

At Sphere Federation, the internet connection is protected with firewalls and multiple layers of security, including a web filtering system called SonicWall and monitoring provided by Impero.

There are three types of appropriate monitoring identified by the Safer Internet Centre. These are:

1. Physical monitoring (adult supervision in the classroom, at all times)
2. Internet and web access
3. Active/Pro-active technology monitoring services

At Sphere Federation, we use a combination of all three to ensure that children are safe when using technology. School devices are monitored and any inappropriate use is reported back to the Federation Safeguarding Lead and the Head of Schools. This monitoring is in effect both at school and when devices are used offsite.

Electronic communications

Please read this section alongside references to pupil-staff communications in the overall school Safeguarding Policy, and in conjunction with the Data Protection Policy. This section only covers electronic communications, but the same principles of transparency, appropriate conduct and audit trail apply.

Email

Staff and pupils within the federation use Gmail for all school emails.

The system is managed by an administrator within the school. This is for the mutual protection and privacy of all staff, pupils and parents, as well as to support data protection. Staff use strict passwords (see page 27). Staff are frequently reminded to activate two-factor authentication upon email set-up.

There are three main school-based electronic systems used to communicate information:

- Email
- School Comms (email and texting service)
- The school website

The school also has official Twitter and Facebook accounts.
Any unauthorised attempt to use a different system may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a child) or to the head of federation (if by a staff member)
General principles for email use are as follows:

- Email may only be sent using an official school email account and only from admin, the Head of School / Head of Federation or a generic email account, eg. for Early Years. There should be no circumstances where a private email is used; if this happens by mistake, the DSL/Head of Federation/DPO (the particular circumstances of the incident will determine whose remit this is) should be informed immediately.
- Teachers or teaching assistants should not enter into an email interchange from their named *@spherefederation.org* account with parents. Instead the office email address

should be used or, when applicable, for example to send digital homework to a teacher, a generic class email address should be used (eg *y2moortown@spherefederation.org*).

- Staff or pupil personal data should never be sent/shared/stored on email unless encrypted with a password. The password should be sent in a separate email.
    - If data needs to be shared with external agencies, EFT encrypted file transfer is used to encrypt data.
- Appropriate behaviour is expected at all times, and the system should not be used to send inappropriate materials or language which is or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which (for staff) might bring the school into disrepute or compromise the professionalism of staff.
- All *@spherefederation.org* users should be aware that emails can be subject to subject access requests – this means that somebody has the right to request access to emails which refer to them.
- Staff are NOT allowed to use the email system for personal use and should be aware that all use is monitored, their emails may be read and the same rules of appropriate behaviour apply at all times. Emails using inappropriate language, images, malware or to adult sites may be blocked and not arrive at their intended destination.

See also the social media section of this policy.

School website

The school website is a key public-facing information portal for the school community with a key reputational value. The Head of Federation / Head of School have the day-to-day responsibility of updating and monitoring the content of the website. The site is managed by Magpie Creative Communications Agency.

Where other staff submit information for the website, they are asked to remember:

- School have the same duty as any person or organisation to respect and uphold copyright law – schools have been fined thousands of pounds for copyright breaches. Sources must always be credited and material only used with permission. There are many open-access libraries of high-quality public-domain images that can be used (e.g. pixabay.com for marketing materials – beware some adult content on this site).
- Where pupil work, images or videos are published on the website, their identities are protected and full names are not published (remember also not to save images with a filename that includes a pupil's full name).

Cloud platforms

Many schools are recognising the benefits of cloud computing platforms, not just for cost savings but to enhance teaching and learning.

This school adheres to the principles of the DfE document 'Cloud computing services: guidance for school leaders, school staff and governing bodies'.

The following principles apply:

- Privacy statements inform parents and children (13+) when and what sort of data is stored in the cloud
- The DPO approves new cloud systems, what may or may not be stored in them and by whom.
- Regular training ensures all staff understand sharing functionality and this is audited to ensure that pupil data is not shared by mistake. Open access or widely shared folders are clearly marked as such
- Staff are only given access and/or sharing rights when they can demonstrate an understanding of what data may be stored and how it can be seen
- Pupil images/videos are only made public with parental permission
- Only school-approved platforms are used by students or staff to store pupil work
- Stakeholders understand the difference between consumer and education products (e.g. a private Gmail account or Google Drive and those belonging to a managed educational domain)

Digital images and video

When a pupil/student joins the school, parents/carers are asked if they give consent for their child's image to be captured in photographs or videos, for what purpose (beyond internal assessment, which does not require express consent) and for how long. Parents answer as follows:

- For use in school
- For the school website
- For use in newspapers
- For social media
- For authorised individuals/companies who have visited school for curriculum events to be used in their own publicity materials
- For use on the school website after their child/children have left the school

Whenever a photo or video is taken/made, the member of staff taking it will check for permission before using it for any purpose.

Any pupils shown in online public facing materials are never identified with a name (and photo file names/tags do not include full names to avoid accidentally sharing them).

All staff are governed by their contract of employment and the school's Acceptable Use Policy, which covers the use of mobile phones/personal equipment for taking pictures of pupils, and where these are stored. Members of staff may occasionally use personal phones to capture photos or videos of pupils, but these will be appropriate, linked to school activities, taken without secrecy (eg by alerting a line manager) and not in a one-to-one situation, and always moved to school storage as soon as possible, after which they are deleted from personal devices or personal cloud services (NB – many phones automatically back up photos).

Photos and videos are only stored on the school's network or the school's cloud system (Google Drive) in line with the retention schedule of the school Data Protection Policy.

Public performances (plays, concerts, assemblies, staff-led learning workshops etc)

Staff and parents are reminded at least annually (eg during an assembly or performance) about the importance of not sharing digital images and video without permission, due to reasons of child protection (e.g. looked-after children often have restrictions for their own protection), data protection, religious or cultural reasons, or simply for reasons of personal privacy.

We appreciate that families will treasure photographic/video memories, and the general rule is that parents and carers may take photos and videos of the children in their care, for personal use only. There may be rare exceptions to this, and parents / carers will be made aware in advance of particular events where no filming etc is possible.

When parents capture footage or still images of their children, there is a strong possibility that other children will also be visible or audible. For this reason, no such content should be shared publicly.

Live streaming, whether public or private, cannot be permitted on streaming platforms or 'live' features (e.g. Facebook Live) to stream events/circumstances as they occur. Parents / carers may be asked to leave the premises or event if this takes place.

Parents will be provided with clear direction by a senior member of staff in order to comply with this content around public performances.

Young people's digital footprint

We encourage young people to think about their online reputation and digital footprint, so we should be good adult role models by not oversharing (or providing embarrassment in later life – and it is not for us to judge what is embarrassing or not). Pupils are taught about how images can be manipulated in their online safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children

Pupils are advised to be very careful about placing any personal photos on social media. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.

Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location. We teach them about the need to keep their data secure and what to do if they / or a friend are subject to bullying or abuse.

Social media

We aim to manage our social media reputation through our website and through our official Facebook and Twitter accounts. We encourage parents / carers to use these channels in order to be more involved in what's happening in school. Parents / carers should not use these

channels to communicate about their children – this is for safeguarding reasons. Similarly, parents / carers should not use these channels to raise a specific concern – we want to be responsive to our community and directly communicating ensures this happens; we may not become aware of the concern they have raised on social media.

Social media (including here all apps, sites and games that allow sharing and interaction between users) is a fact of modern life, and as a school, we accept that many parents, staff and pupils will use it. However, as stated in the acceptable use policies which all members of the school community should adhere to, we expect everybody to behave in a positive manner, engaging respectfully with the school and each other on social media, in the same way as they would face to face.

This positive behaviour can be summarised as not making any posts which are or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which might bring the school or (particularly for staff) teaching profession into disrepute. This applies both to public pages and to private posts, e.g. parent chats, pages or groups.

If parents have a concern about the school, we would urge them to contact us directly and in private to resolve the matter. If an issue cannot be resolved in this way, the school complaints procedure should be followed. Sharing complaints on social media is unlikely to help resolve the matter, but can cause upset to staff, pupils and parents, also undermining staff morale and the reputation of the federation (which is important for the pupils we serve).

Many social media platforms have a minimum age of 13, but the federation is increasingly dealing with issues arising on social media with pupils under the age of 13. We ask parents to respect age ratings on social media platforms wherever possible and not encourage or condone underage use. It is worth noting that following on from the government's Safer Internet Strategy, enforcement and age checking is likely to become more stringent over the coming years.

The federation has to strike a difficult balance of not encouraging underage use at the same time as needing to acknowledge reality in order to best help our pupils to avoid or cope with issues if they arise. Online safety lessons will look at social media and other online behaviour, how to be a good friend online and how to report bullying, misuse, intimidation or abuse. However, children will often learn most from the models of behaviour they see and experience, which will often be from adults.

Parents can best support this (Parents' responsibilities as outlined on p.13) by talking to their children about the apps, sites and games they use (you don't need to know them – ask your child to explain it to you), with whom, for how long, and when (late at night / in bedrooms is not helpful for a good night's sleep and productive teaching and learning at school the next day). You may wish to introduce the Children's Commission Digital 5 A Day.

It is encouraging that 73% of pupils (from the 40,000 who answered that LGfL DigiSafe pupil online safety survey) trust their parents on online safety (although only half talk about it with them more than once a year at the moment).

Pupils are not allowed* to be 'friends' with or make a friend request** to any staff, governors, volunteers and contractors or otherwise communicate via social media.

Pupils are discouraged from 'following' staff, governor, volunteer or contractor public accounts (e.g. following a staff member with a public Instagram account). However, we accept that this can be hard to control (but this highlights the need for staff to remain professional in their private lives). In the reverse situation, however, staff must not follow such public student accounts.

* Exceptions may be made, e.g. for pre-existing family links, but these must be approved by the Head of School, and should be declared upon entry of the pupil or staff member to the school).

** Any attempt to do so may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a child) or to the Head of Federation (if by a staff member).

Staff are reminded that they are obliged not to bring the school or profession into disrepute and the easiest way to avoid this is to have the strictest privacy settings and avoid inappropriate sharing and oversharing online. New members of staff should review their social media accounts when they join the school to check that published content is accurate and appropriate and that privacy settings are strict. Staff should not identify themselves as representatives of the school and never discuss the school or its stakeholders on social media. They need to be careful that their personal opinions might not be attributed to the school or local authority, bringing the school into disrepute.

The serious consequences of inappropriate behaviour on social media are underlined by the fact that there have been 200 Prohibition Orders issued to teachers over the past four years related to the misuse of technology/social media.

All members of the school community are reminded that particularly in the context of social media, it is important to comply with the school policy on Digital Images and Video (see page 23) and permission is sought before uploading photographs, videos or any other information about other people.

The statements of the Acceptable Use Policies (AUPs) which all members of the school community have agreed to follow are also relevant to social media activity, as is the school's Data Protection Policy.

Device usage

Please read the following in conjunction with acceptable use policies and the following sections of this document which all impact upon device usage: copyright, data protection, social media, misuse of technology, and digital images and video.

Personal devices including wearable technology

- **Pupils** in key stage 2 may bring mobile phones into school (typically these are children who walk to and/or from school by themselves) but they must be handed into the school office when they arrive. The phones are switched off and kept in a secure place until the children collect them at the end of the school day. Important messages and phone calls to or from parents can be made at the school office which will also pass on messages from parents to pupils in emergencies. Pupils' personal devices are not able to connect to the school network or internet.

- **All staff who work directly with children** should leave their mobile phones on silent and only use them in private staff areas (eg to make calls, check personal emails) during school hours or in a very public space (eg to use a calculator, to check the time) where other adults are present. See also the Digital images and video section on page 23 and Data protection and data security section on page 20. Child/staff data should never be downloaded onto a private phone. If a staff member is expecting an important personal call when teaching or otherwise on duty, they should ask permission to keep their phones on vibrate so they can take the call in a private area. Personal devices must be password protected. If using the school internet for personal use during a break, staff members must ensure that usage is not in any way inappropriate for an education setting. The same is true for members of staff using mobile data on a personal device on school premises.
  Staff may use personal devices to check work emails both on and off the school premises but, as mentioned, earlier, the device must be password protected.
- **Volunteers, contractors, governors** should leave their phones in their pockets and on silent. Under no circumstances should they be used in the presence of children or to take photographs or videos. If this is required (e.g. for contractors to take photos of equipment or buildings), permission of the Head of School should be sought (the Head of School may choose to delegate this) and this should be done in the presence of a member of staff. Volunteers, contractors or governors will not be given school network or internet access on personal devices.
- **Parents** are asked to leave their phones in their pockets when they are on site. They should ask permission before taking any photos, eg of displays in corridors or classrooms, and avoid capturing other children. When at school events, please refer to the Digital images and video section of this document on page 23. Parents are asked not to call pupils on their mobile phones during the school day; urgent messages can be passed via the school office. Parents will not be given school network or internet access on their personal devices.

Network / internet access on school devices

- **Pupils/students** will often use school devices during lessons or, on occasion, during break times or after school. All pupils have an individual username and password to access the school network and should always log off devices when they have finished using them. Whilst at school, pupils will access the internet using school devices. They are aware that this use is monitored and any misuse will be dealt with in line with the school's relationships policy.
- **Members of staff** use strong passwords to access the school network. To protect themselves, they should lock devices if they step away from them. When they have finished using a school device, they should make sure they log off securely. Some members of staff take devices off-site. Personal use of these devices is allowed but staff members are aware that usage is monitored and any misuse will be dealt with as outlined in the staff handbook.
- **Volunteers, contractors, governors** will not typically use school devices to access the school network or internet but, if agreed with the Head of School, may use a school device in the presence of a member of staff.

- **Parents** will not normally have access to school devices (they would be heavily supervised if given access).

Trips / events away from school

For school trips/events away from school, teachers may be issued a school duty phone and this number used for any authorised or emergency communications with parents. Any deviation from this policy (e.g. by mistake or because the school phone will not work or is unavailable) will be notified immediately to the head of school. Teachers using their personal phone will ensure that the number is hidden to avoid a parent or student accessing a teacher's private phone number.

Searching and confiscation

In line with the DfE guidance 'Searching, screening and confiscation: advice for schools', the Head of Federation and staff authorised by them have a statutory power to search pupils' property on school premises. This includes the content of mobile phones and other devices, for example as a result of a reasonable suspicion that a device contains illegal or undesirable material, including but not exclusive to sexual images, pornography, violence or bullying.

Appendices

1. Acceptable Use Policy (AUP) for KS1
2. Acceptable Use Policy (AUP) for KS2
3. Acceptable Use Policy (AUP) for parents/carers
4. Acceptable Use Policy (AUP) for staff

Online Safety

KS1 Acceptable Use Policy

SCHOLES
Scholes (Elmet) Primary School

My name is_____

To stay **SAFE online and on my devices**:	✓
1. I only **use** devices or apps, sites or games if a trusted adult says so.	
2. I **ask** for help if I'm stuck or not sure.	
3. I **tell** a trusted adult if I'm upset, worried, scared or confused.	
4. If I get a **funny feeling** in my tummy, I talk to an adult.	
5. I look out for my **friends** and tell someone if they need help.	
6. I **know** people online aren't always who they say they are.	
7. Anything I do online can be shared and might stay online **forever**.	
8. I don't keep **secrets** or do **dares and challenges** just because someone tells me I have to.	
9. I don't change **clothes** in front of a camera.	
10. I always check with an adult before **sharing** personal information.	
11. I am **kind** and polite to everyone.	

My trusted adults at **school** are:	My trusted adults at **home** are:

Online Safety

KS1 Acceptable Use Policy

My name is_____

To stay **SAFE online and on my devices**:	✓
1. I only **use** devices or apps, sites or games if a trusted adult says so.	
2. I **ask** for help if I'm stuck or not sure.	
3. I **tell** a trusted adult if I'm upset, worried, scared or confused.	
4. If I get a **funny feeling** in my tummy, I talk to an adult.	
5. I look out for my **friends** and tell someone if they need help.	
6. I **know** people online aren't always who they say they are.	
7. Anything I do online can be shared and might stay online **forever**.	
8. I don't keep **secrets** or do **dares and challenges** just because someone tells me I have to.	
9. I don't change **clothes** in front of a camera.	
10. I always check with an adult before **sharing** personal information.	
11. I am **kind** and polite to everyone.	

My trusted adults at **school** are:	My trusted adults at **home** are:

Online Safety

ST JAMES' Church of England Primary School

KS1 Acceptable Use Policy

My name is_____

To stay **SAFE online and on my devices**:	✓
1. I only **use** devices or apps, sites or games if a trusted adult says so.	
2. I **ask** for help if I'm stuck or not sure.	
3. I **tell** a trusted adult if I'm upset, worried, scared or confused.	
4. If I get a **funny feeling** in my tummy, I talk to an adult.	
5. I look out for my **friends** and tell someone if they need help.	
6. I **know** people online aren't always who they say they are.	
7. Anything I do online can be shared and might stay online **forever**.	
8. I don't keep **secrets** or do **dares and challenges** just because someone tells me I have to.	
9. I don't change **clothes** in front of a camera.	
10. I always check with an adult before **sharing** personal information.	
11. I am **kind** and polite to everyone.	

My trusted adults at **school** are:	My trusted adults at **home** are:

Online Safety

KS2 Acceptable Use Policy

SCHOLES
Scholes (Elmet) Primary School

Name:

This agreement will help keep me safe and help me to be fair to others.

1. **I learn online.** I use the school's internet and devices for schoolwork and other activities to learn and have fun. School internet and devices are monitored.
2. **I ask permission.** Whether at home or school, I only use the devices, apps, sites and games I am allowed to, at the times I am allowed to.
3. **I am creative online.** I don't just spend time on apps, sites and games looking at things from other people. I get creative to learn and make things.
4. **I am a friend online.** I won't share anything that I know another person wouldn't want shared, or which might upset them. If I know a friend is worried or needs help, I will remind them to talk to an adult, or even do it for them.
5. **I am a secure online learner.** I keep my passwords to myself and reset them if anyone finds them out. Friends don't share passwords!
6. **I am careful what I click on.** I don't click on unexpected links or popups, and only download or install things when I know it's safe or has been agreed by trusted adults. Sometimes, add-ons can cost money, so it's important I always check for these, too.
7. **I ask for help if I am scared or worried.** I will talk to a trusted adult if anything upsets me or worries me on an app, site or game – it often helps. If I get a funny feeling, I talk about it.
8. **I know it's not my fault if I see or someone sends me something bad.** I won't get in trouble, but I mustn't share it. Instead, I will tell a trusted adult. If I make a mistake, I don't try to hide it but ask for help.
9. **I communicate and collaborate online** …with people I already know and have met in real life or that a trusted adult knows about.
10. **I know new online friends might not be who they say they are.** I am careful when someone wants to be my friend. Unless I have met them face to face, I can't be sure who they are.
11. **I check with an adult before I meet an online friend** …face to face for the first time, and I never go alone.
12. **I don't do live videos (livestreams) on my own** …and always check if it's allowed. I check with a trusted adult before I video chat with anybody for the first time.
13. **I keep my body to myself online.** I never get changed or show what's under my clothes in front of a camera. I remember my body is mine and no-one should tell me what to do with it; I don't send any photos or videos without checking with a trusted adult.

14. **I say no online if I need to.** I don't have to do something just because a friend dares or challenges me to do it, or to keep a secret. If I get asked anything that makes me worried, upset or just confused, I should say no, stop chatting and tell a trusted adult immediately.
15. **I tell my parents/carers what I do online.** They might not know the app, site or game, but they can still help me when things go wrong, and they want to know what I'm doing.
16. **I am private online.** I only give out private information if a trusted adult says it's ok. This might be my address, phone number, location or anything else that could identify me or my family and friends; if I turn on my location, I will remember to turn it off again.
17. **I am careful what I share and protect my online reputation.** I know anything I do can be shared and might stay online forever (even on Snapchat or if I delete it).
18. **I am a rule-follower online.** I know that apps, sites and games have rules on how to behave, and some have age restrictions. I follow the rules, block bullies and report bad behaviour.
19. **I am not a bully.** I do not post, make or share unkind, hurtful or rude messages/comments and if I see it happening, I will tell my trusted adults.
20. **I am part of a community.** I do not make fun of anyone or exclude them because they are different to me. If I see anyone doing this, I tell a trusted adult.
21. **I respect people's work.** I only edit or delete my own digital work and only use words, pictures or videos from other people if I have their permission or if it is copyright free or has a Creative Commons licence.
22. **I am a researcher online.** I use safe search tools approved by my trusted adults. I know I can't believe everything I see online, know which sites to trust, and know how to double check information I find.

I have read and understood this agreement.	
If I have any questions at school, I will speak to a trusted adult:	**Outside school, my trusted adults are**
Signed:	**Date:**

Online Safety

KS2 Acceptable Use Policy

Name:

This agreement will help keep me safe and help me to be fair to others.

1. **I learn online.** I use the school's internet and devices for schoolwork and other activities to learn and have fun. School internet and devices are monitored.
2. **I ask permission.** Whether at home or school, I only use the devices, apps, sites and games I am allowed to, at the times I am allowed to.
3. **I am creative online.** I don't just spend time on apps, sites and games looking at things from other people. I get creative to learn and make things.
4. **I am a friend online.** I won't share anything that I know another person wouldn't want shared, or which might upset them. If I know a friend is worried or needs help, I will remind them to talk to an adult, or even do it for them.
5. **I am a secure online learner.** I keep my passwords to myself and reset them if anyone finds them out. Friends don't share passwords!
6. **I am careful what I click on.** I don't click on unexpected links or popups, and only download or install things when I know it's safe or has been agreed by trusted adults. Sometimes, add-ons can cost money, so it's important I always check for these, too.
7. **I ask for help if I am scared or worried.** I will talk to a trusted adult if anything upsets me or worries me on an app, site or game – it often helps. If I get a funny feeling, I talk about it.
8. **I know it's not my fault if I see or someone sends me something bad.** I won't get in trouble, but I mustn't share it. Instead, I will tell a trusted adult. If I make a mistake, I don't try to hide it but ask for help.
9. **I communicate and collaborate online** …with people I already know and have met in real life or that a trusted adult knows about.
10. **I know new online friends might not be who they say they are.** I am careful when someone wants to be my friend. Unless I have met them face to face, I can't be sure who they are.
11. **I check with an adult before I meet an online friend** …face to face for the first time, and I never go alone.
12. **I don't do live videos (livestreams) on my own** …and always check if it's allowed. I check with a trusted adult before I video chat with anybody for the first time.
13. **I keep my body to myself online.** I never get changed or show what's under my clothes in front of a camera. I remember my body is mine and no-one should tell me

what to do with it; I don't send any photos or videos without checking with a trusted adult.

14. **I say no online if I need to.** I don't have to do something just because a friend dares or challenges me to do it, or to keep a secret. If I get asked anything that makes me worried, upset or just confused, I should say no, stop chatting and tell a trusted adult immediately.
15. **I tell my parents/carers what I do online.** They might not know the app, site or game, but they can still help me when things go wrong, and they want to know what I'm doing.
16. **I am private online.** I only give out private information if a trusted adult says it's ok. This might be my address, phone number, location or anything else that could identify me or my family and friends; if I turn on my location, I will remember to turn it off again.
17. **I am careful what I share and protect my online reputation.** I know anything I do can be shared and might stay online forever (even on Snapchat or if I delete it).
18. **I am a rule-follower online.** I know that apps, sites and games have rules on how to behave, and some have age restrictions. I follow the rules, block bullies and report bad behaviour.
19. **I am not a bully.** I do not post, make or share unkind, hurtful or rude messages/comments and if I see it happening, I will tell my trusted adults.
20. **I am part of a community.** I do not make fun of anyone or exclude them because they are different to me. If I see anyone doing this, I tell a trusted adult.
21. **I respect people's work.** I only edit or delete my own digital work and only use words, pictures or videos from other people if I have their permission or if it is copyright free or has a Creative Commons licence.
22. **I am a researcher online.** I use safe search tools approved by my trusted adults. I know I can't believe everything I see online, know which sites to trust, and know how to double check information I find.

I have read and understood this agreement.	
If I have any questions at school, I will speak to a trusted adult:	**Outside school, my trusted adults are**

Signed:	**Date:**

Online Safety

KS2 Acceptable Use Policy

ST JAMES' Church of England Primary School

Name:

This agreement will help keep me safe and help me to be fair to others.

1. **I learn online.** I use the school's internet and devices for schoolwork and other activities to learn and have fun. School internet and devices are monitored.
2. **I ask permission.** Whether at home or school, I only use the devices, apps, sites and games I am allowed to, at the times I am allowed to.
3. **I am creative online.** I don't just spend time on apps, sites and games looking at things from other people. I get creative to learn and make things.
4. **I am a friend online.** I won't share anything that I know another person wouldn't want shared, or which might upset them. If I know a friend is worried or needs help, I will remind them to talk to an adult, or even do it for them.
5. **I am a secure online learner.** I keep my passwords to myself and reset them if anyone finds them out. Friends don't share passwords!
6. **I am careful what I click on.** I don't click on unexpected links or popups, and only download or install things when I know it's safe or has been agreed by trusted adults. Sometimes, add-ons can cost money, so it's important I always check for these, too.
7. **I ask for help if I am scared or worried.** I will talk to a trusted adult if anything upsets me or worries me on an app, site or game – it often helps. If I get a funny feeling, I talk about it.
8. **I know it's not my fault if I see or someone sends me something bad.** I won't get in trouble, but I mustn't share it. Instead, I will tell a trusted adult. If I make a mistake, I don't try to hide it but ask for help.
9. **I communicate and collaborate online** …with people I already know and have met in real life or that a trusted adult knows about.
10. **I know new online friends might not be who they say they are.** I am careful when someone wants to be my friend. Unless I have met them face to face, I can't be sure who they are.
11. **I check with an adult before I meet an online friend** …face to face for the first time, and I never go alone.
12. **I don't do live videos (livestreams) on my own** …and always check if it's allowed. I check with a trusted adult before I video chat with anybody for the first time.
13. **I keep my body to myself online.** I never get changed or show what's under my clothes in front of a camera. I remember my body is mine and no-one should tell me what to do with it; I don't send any photos or videos without checking with a trusted adult.

14. **I say no online if I need to.** I don't have to do something just because a friend dares or challenges me to do it, or to keep a secret. If I get asked anything that makes me worried, upset or just confused, I should say no, stop chatting and tell a trusted adult immediately.
15. **I tell my parents/carers what I do online.** They might not know the app, site or game, but they can still help me when things go wrong, and they want to know what I'm doing.
16. **I am private online.** I only give out private information if a trusted adult says it's ok. This might be my address, phone number, location or anything else that could identify me or my family and friends; if I turn on my location, I will remember to turn it off again.
17. **I am careful what I share and protect my online reputation.** I know anything I do can be shared and might stay online forever (even on Snapchat or if I delete it).
18. **I am a rule-follower online.** I know that apps, sites and games have rules on how to behave, and some have age restrictions. I follow the rules, block bullies and report bad behaviour.
19. **I am not a bully.** I do not post, make or share unkind, hurtful or rude messages/comments and if I see it happening, I will tell my trusted adults.
20. **I am part of a community.** I do not make fun of anyone or exclude them because they are different to me. If I see anyone doing this, I tell a trusted adult.
21. **I respect people's work.** I only edit or delete my own digital work and only use words, pictures or videos from other people if I have their permission or if it is copyright free or has a Creative Commons licence.
22. **I am a researcher online.** I use safe search tools approved by my trusted adults. I know I can't believe everything I see online, know which sites to trust, and know how to double check information I find.

I have read and understood this agreement.	
If I have any questions at school, I will speak to a trusted adult:	**Outside school, my trusted adults are**
Signed:	**Date:**

Scholes (Elmet) Primary
St James' CE Primary
Moortown Primary

Online safety:
Acceptable use policy for parents/carers

What is an acceptable use policy?

We ask all children, young people and adults involved in the life of Sphere Federation to adhere to an Acceptable Use Policy (AUP), which is a document that outlines how we expect them to behave when they are online, and/or using school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).

Why do we need an AUP?

These rules have been written to help keep everyone safe and happy when they are online or using technology. Sometimes things go wrong and people can get upset, but these rules should help us avoid it when possible, and be fair to everybody.

School systems and users are protected and monitored by security and filtering services to provide safe access to digital technologies. This means anything on a school device or using school networks/platforms/internet may be viewed by one of the staff members who are here to keep your children safe.

We tell your children that they should not behave any differently when they are out of school or using their own device or home network. What we tell pupils about behaviour and respect applies to all members of the school community:
'Treat yourself and others with respect at all times; treat people in the same way when you are online or on a device as you would face to face.'

Where can I find out more?

You can read Sphere Federation's full Online Safety Policy for more detail on our approach to online safety and links to other relevant policies (eg Safeguarding Policy, Behaviour Policy, etc). If you have any questions about this AUP or our approach to online safety, please speak to the Head of School.

What am I agreeing to?

1. I understand that Sphere Federation uses technology as part of the daily life of the school when it is appropriate to support teaching & learning and the smooth running of the school, and to help prepare the children and young people in our care for their future lives.

2. I understand that the school takes every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. These precautions include the relationship policy and acceptable use agreements, physical and technical monitoring, education and support and web filtering. However, the school cannot be held responsible for the nature and content of materials accessed through the internet and mobile technologies, which can sometimes be upsetting.

3. I understand that internet and device use in school is subject to filtering and monitoring.

4. I will promote positive online safety and model safe, responsible and positive behaviours in my own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers.

5. The impact of social media use is often felt strongly in schools, which is why we expect certain behaviours from pupils when using social media. I will support the school's online safety policy in regard to social media and not encourage my child to join any platform where they are below the minimum age.

6. I will follow the school's online safety policy, which outlines when I can capture and/or share images/videos. I will not share images of other people's children on social media and understand that there may be cultural or legal reasons why this would be inappropriate or even dangerous. The school sometimes uses images/video of my child for internal purposes such as recording attainment, but it will only do so publicly if I have given my consent on the relevant form.

7. I understand that for my child to grow up safe online, they will need positive input from school and home, so I will talk to my child about online safety (NB: the recent LGfL DigiSafe survey of 40,000 primary and secondary pupils found that 73% of pupils trust their parents on online safety, but only half talk about it with them more than once a year). Understanding human behaviour is more helpful than knowing how a particular app, site or game works.

8. I understand that whilst home networks are much less secure than school ones, I can apply child safety settings to my home internet. Internet Matters provides guides to help parents do this easily for all the main internet service providers in the UK.

9. I understand that it can be hard to stop using technology sometimes, and I will talk about this to my children, and refer to the principles of the Digital 5 A Day: childrenscommissioner.gov.uk/our-work/digital/5-a-day/

10. I understand and support the commitments made by my child in the Acceptable Use Policy (AUP) and I understand that they will be subject to sanctions if they do not follow these rules.

11. I can find out more about online safety at Sphere Federation by reading the full Online Safety Policy and can talk to the Head of School if I have any concerns about my child/ren's use of technology or if I have questions about online safety or technology use in school.

Scholes (Elmet) Primary
St James' CE Primary
Moortown Primary

Online safety:
Acceptable use policy for staff

What is an acceptable use policy?

We ask all children, young people and adults involved in the life of Sphere Federation to adhere to an Acceptable Use Policy (AUP), which outlines how we expect them to behave when they are online, and/or using school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).
This AUP is reviewed annually, and I will be asked to sign it upon entry to the school and every time changes are made.

Why do we need an AUP?

All staff and governors have particular legal / professional obligations and it is imperative that all parties understand that online safety is part of safeguarding as well as part of the curriculum, and it is everybody's responsibility to uphold the school's approaches, strategy and policy as detailed in the full Online Safety Policy.

Where can I find out more?

All staff, governors and volunteers should read Sphere Federation's full Online Safety Policy for more detail on our approach to online safety and links to other relevant policies (eg Safeguarding Policy, Positive Relationships Policy, etc).
If you have any questions about this AUP or our approach to online safety, please speak to the Head of Federation or the Head of School.

What am I agreeing to?

1. I have read and understood Sphere Federation's full Online Safety Policy and agree to uphold the spirit and letter of the approaches outlined there, both for my behaviour as an adult and enforcing the rules for pupils. I will report any breaches or suspicions (by adults or children) in line with the policy without delay.

2. I understand it is my duty to support a whole-school safeguarding approach and will report any behaviour which I believe may be inappropriate or concerning in any way to the Designated Safeguarding Lead (if by a child) or the Head of Federation (if by an adult).

3. I understand the responsibilities listed for my role in the school's Online Safety policy (staff please note that the 'all staff' section applies as well as any other category) and agree to abide by these.

4. I understand that school systems and users are protected by security, monitoring and filtering services, and that my use of school devices (regardless of time, location or internet connection) and networks/platforms/internet/other technologies, including encrypted content, is monitored/captured/viewed by these systems and/or relevant/authorised staff members.

5. I understand that I am a role model and will promote positive online safety and model safe, responsible and positive behaviours in my own use of technology, including social media, eg by:

- not sharing other's images or details without permission
- refraining from posting negative, threatening or violent comments about others, regardless of whether they are members of the school community or not.

6. I will not contact or attempt to contact any pupil or to access their contact details (including their usernames/handles on different platforms) in any way other than school-approved and school-monitored ways, which are detailed in the school's Online Safety Policy. I will report any breach of this by others or attempts by pupils to do the same to the Head of Federation.

7. Details on social media behaviour, the general capture of digital images/video and on my use of personal devices is stated in the full Online Safety Policy. If I am not sure if I am allowed to do something in or related to school, I will not do it.

8. I understand the importance of upholding my online reputation, my professional reputation and that of the school, and I will do nothing to impair either.

9. I agree to adhere to all provisions of the school Data Protection Policy at all times, whether or not I am on site or using a school device, platform or network, and will ensure I do not access, attempt to access, store or share any data which I do not have express permission for. I will protect my passwords/logins and other access, never share credentials and immediately change passwords and notify the head of school if I suspect a breach. I will not store school-related data on personal devices, storage or cloud platforms. USB keys, where allowed, will be encrypted, and I will only use safe and appropriately licensed software, respecting licensing, intellectual property and copyright rules at all times.

10. I will use school devices and networks/internet/platforms/other technologies for school business appropriately and I will never use these to access material that is illegal or in any way inappropriate for an education setting. I will not attempt to bypass security or monitoring and will look after devices loaned to me.

11. I will not support or promote extremist organisations, messages or individuals, nor give them a voice or opportunity to visit the school. I will not browse, download or send material that is considered offensive or of an extremist nature by the school.

12. I understand and support the commitments made by pupils, parents and fellow staff, governors and volunteers in their Acceptable Use Policies and will report any infringements in line with school procedures.

13. I will follow the guidance in the Online Safety Policy for reporting incidents – I understand the principle of 'safeguarding as a jigsaw' where my concern might complete the picture. I have read the sections on handing incidents and concerns about a child in general, sexting, upskirting, bullying, sexual violence and harassment, misuse of technology and social media.

14. I understand that breach of this AUP and/or of the school's full Online Safety Policy here may lead to appropriate staff disciplinary action or termination of my relationship with the school and where appropriate, referral to the relevant authorities.