



Flourish FEDERATION

Believe, Achieve, Belong



Online Policy



The Flourish Federation Vision

To inspire everyone to flourish, grow and learn in a safe and spiritually rich environment.

Built on the strong foundations of Matthew 7:24

Everyone then who hears these words of mine and does them will be like a wise man who built his house on the rock.

Our Federation's vision, ethos and Christian values underpin and thread through every aspect of our work across our Federation. Our work helps us on our collective journey to achieve our vision for all in our Federation community.

This policy was ratified by Flourish Federation Governing Body on:	1st Feb 2024
This policy will be reviewed by Flourish Federation Governing Body on: (unless earlier review is required to adhere to statutory requirements/changes in procedure)	1st Feb 2025
Policy Version:	v
Signed by the Chair of Governors:	
Signed by the Executive Headteacher:	

Our Values



The headteacher has an overview of online safety.
Our Online Safety Policy is based on national educational trust guidelines

The online safety policy will be reviewed annually or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place.

The federation and ICT solutions will monitor the impact of the policy Logs of reported incidents

- Monitoring logs of internet activity (including sites visited)
- Internal monitoring data for network activity
- Surveys/questionnaires of
 - Pupils/students
 - Parents/carers
 - Staff

Scope of the Policy

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

The Education and Inspections Act (2006) empowers Headteachers to such an extent as is reasonable, to regulate the behaviour of pupils/students 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 outside of the school, but is linked to membership of the federation. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (See Appendix 7). In the case of both acts, action can only be taken over issues covered by the federation Behaviour/Relationship Policy.

The federation will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of the federation.

Roles and Responsibilities

The local governing body (LGB) are responsible for the approval of the online safety policy. The LGB are responsible for monitoring the implementation of this policy. This will be carried out by the LGB receiving regular information about online safety incidents and monitoring reports. A member of the LGB has taken on the role of online safety Governor (Safeguarding governor?) and the role includes:

- regular meetings with the Headteacher or Business Manager
- regular monitoring of online safety incident logs
- regular monitoring of filtering/change control logs
- reporting to LGB

Headteacher/Principal and Senior Leaders

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the federation community, though the day-to-day responsibility for online safety will be delegated to the online safety lead.
- The Headteacher and (at least) another member of the Senior Leadership/Senior Management Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff

- The Headteacher/Senior Leaders are responsible for ensuring that the online safety Coordinator and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Headteacher/Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in the federation who carry out the internal online safety monitoring role. This is to provide a safety net and also support those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive regular monitoring reports from the online safety Lead

Online safety lead (ICT leader)

- Leads the online safety
- Takes day to day responsibility for online safety issues and has a leading role in establishing and review the federation online safety policies/documents
- Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- Provides training and advice for staff
- Liaises with the Headteacher or LGB
- Liaises with federation technical staff
- Receives reports of online safety incidents and creates a log of incidents to inform future online safety developments.
- Meets regularly with online safety Governor to discuss current issues. Review incident logs and filtering/change control logs
- Attends relevant meeting/committee of LGB
- Reports regularly to Senior Leadership Team

ICT Coordinator/ICT solutions is responsible for ensuring

- That the federation's technical infrastructure is secure and is not open to misuse or malicious attack
- that the federation meets required online safety technical requirements
- That users may only access the networks and devices through a properly enforced password protection policy.
- the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- That they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- That the use of the network / internet / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher
- That monitoring software / systems are implemented and updated as agreed in federation policies

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up-to-date awareness of online safety matters and of the current federation online safety policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)
- They report any suspected misuse or problem to the Headteacher
- All digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official federation systems
- online safety issues are embedded in all aspects of the curriculum and other activities

- Pupils/students understand and follow the online safety and acceptable use policies
- Pupils/students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other federation activities (where allowed) and implement current policies with regard to these devices
- In lessons where internet use is pre-planned pupils/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

Designated Safeguarding Lead / Child Protection Officer

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

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

Pupils/Students:

- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- Should understand the importance of adopting good online safety practice when using digital technologies out of federation and realise that the federation's Online safety Policy covers their actions out of the federation, if related to their membership of the federation

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. The federation will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website / VLE and information about national / local online safety campaigns / literature. Parents and carers will be encouraged to support the federation in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at federation events (see Use of Digital Images and Videos policy guidelines below)
- access to parents' sections of the website / VLE and on-line student / pupil records
- their children's personal devices in the federation (where this is allowed)

Policy Statements

Education – students / pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating students / pupils to take a responsible approach. The education of students / pupils in online safety is therefore an essential part of the federation's online safety provision. Children and young people need the help and support of the federation to recognise and avoid online safety risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited
- Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- Students / pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Students / pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students / pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- Students / pupils should be helped to understand the need for the student / pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside federation
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices
- in lessons where internet use is pre-planned, it is best practice that students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where students / pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Education – parents / carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The federation will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, web site, VLE
- Parents / Carers evenings / sessions
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications

www.saferinternet.org.uk/ <http://www.childnet.com/parents-and-carers> ThinkUknow

Education – The Wider Community

The federation will provide opportunities for local community groups / members of the community to gain from the federation's online safety knowledge and experience. This may be offered through the following:

- Providing family learning courses in use of new digital technologies, digital literacy and online safety
- Online safety messages targeted towards grandparents and other relatives as well as parents.
- The federation website will provide online safety information for the wider community
- Supporting community groups e.g. Early Years Settings, Childminders, youth / sports / voluntary groups to enhance their online safety provision

Education & Training – Staff / Volunteers

A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly. It is expected that some staff will identify online safety as a training need within the performance management process.

- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the federation online safety policy and Acceptable Use Agreements. .
- The Online safety Coordinator / Officer (or other nominated person) will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- This Online safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The Online safety Coordinator / Officer (or other nominated person) will provide advice / guidance / training to individuals as required.

Training – Governors

Governors should take part in online safety training / awareness sessions, with particular importance for those who are members of any subcommittee / group involved in technology / online safety / health and safety / child protection. This may be offered in a number of ways:

- Attendance at training provided by the Trust/NGA / National Governors Association / or other relevant organisation.
- Participation in federation training / information sessions for staff or parents (this may include attendance at assemblies / lessons).

Use of Digital Imaging Technologies

The development of digital imaging technologies has created significant benefits to learning allowing staff and students/pupils instant use of images that they have recorded themselves of or downloaded from the internet. Images may also be used to celebrate success through their publication in newsletters, on the federation website and occasionally in the public media,

However, staff, parents, carers and pupils/students need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The federation will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate students / pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In

particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

- Written permission from parents or carers will be obtained before photographs of students / pupils are published on the federation website / social media / local press

In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at federation events for their own personal use (as such use is not covered by the General Data Protection Regulations). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images.

Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow federation policies concerning the sharing, distribution and publication of those images. Those images should only be taken on federation equipment, the personal equipment of staff should not be used for such purposes.

Care should be taken when taking digital / video images that students / pupils are appropriately dressed and are not participating in activities that might bring the individuals or the federation into disrepute.

Students / pupils must not take, use, share, publish or distribute images of others without their permission

Photographs published on the website, or elsewhere that include students / pupils will be selected carefully and will comply with good practice guidance on the use of such images. Students' / Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

Student's / Pupil's work can only be published with the permission of the student / pupil and parents or carers.

Parents / carers will be required to sign a relevant permission form to allow the federation to take and use images of their children and for the parents / carers to agree

The federation will be responsible for ensuring that the federation infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

- Federation technical systems will be managed in ways that ensure that the federation meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of federation technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to federation technical systems and devices.
- All users (at KS2 and above) will be provided with a username and secure password by their class teacher who will keep an up-to-date record of users and their usernames. Users are responsible for the security of their username and password.

- ICT solutions/The headteacher is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations (Inadequate licencing could cause the federation to breach the Copyright Act which could result in fines or unexpected licensing costs)
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes.
- Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet.
- The federation has provided enhanced / differentiated user-level filtering (allowing different filtering levels for different ages / stages and different groups of users – staff / pupils / students etc.)
- Federation technical staff regularly monitors and record the activity of users on the federation technical systems and users are made aware of this in the Acceptable Use Agreement

Mobile Technologies (including Bring Your Own Device BYOD/ Technology BYOT)

Mobile technology devices may be federation owned/provided or personally owned and might include: smartphone, tablet, notebook / laptop or other technology that usually has the capability of utilising the federation's wireless network. The device then has access to the wider internet which may include the federation's learning platform and other cloud-based services such as email and data storage.

- The federation has a set of clear expectations and responsibilities for all users
- The federation adheres to the General Data Protection Regulation principles
- All users are provided with and accept the Acceptable Use Agreement
- All network systems are secure and access for users is differentiated
- Where possible these devices will be covered by the federation's normal filtering systems, while being used on the premises
- All users will use their username and password and keep this safe
- Mandatory training is undertaken for all staff
- Students / Pupils receive training and guidance on the use of personal devices
- Regular audits and monitoring of usage will take place to ensure compliance
- Any device loss, theft, change of ownership of the device will be reported as in the BYOD policy
- Any user leaving the federation will follow the process outlined within the BYOD policy

Data Protection

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.

Please see Data Protection policy

When personal data is stored on any mobile device or removable media the:

- data must be encrypted and password protected.
- device must be password protected. (be sure to select devices that can be protected in this way)

- device must be protected by up to date virus and malware checking software
- data must be securely deleted from the device, in line with school/federation policy (below) once it has been transferred or its use is complete.

Staff must ensure that they:

- at all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- can recognise a possible breach, understand the need for urgency and know who to report it to within the school
- can help data subjects understand their rights and know how to handle a request whether verbal or written. Know who to pass it to in the school
- where personal data is stored or transferred on mobile or other devices (including USBs) these must be encrypted and password protected.
- will not transfer any federation personal data to personal devices except as in line with school policy
- access personal data sources and records only on secure password protected computers and other devices, ensuring that they are properly “logged-off” at the end of any session in which they are using personal data

Communications

This is an area of rapidly developing technologies and uses. Federation’s will need to discuss and agree how they intend to implement and use these technologies eg some federation’s do not allow students / pupils to use mobile phones in lessons, while others recognise their educational potential and allow their use. This section may also be influenced by the age of the students / pupils.

When using communication technologies, the federation considers the following as good practice:

- The official federation email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and students / pupils should therefore use only the federation email service to communicate with others when in the federation, or on federation systems (e.g. by remote access).
- Users must immediately report, to the nominated person – in accordance with the federation policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication. This includes any communication linked to Prevent Duty and radicalisation and linked to child sexual exploitation that can occur through the use of technology.
- Any digital communication between staff and students / pupils or parents / carers (email, chat, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) federation systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Whole class / group email addresses may be used at KS1, while students / pupils at KS2 and above can be provided with individual federation email addresses for educational use.
- Students / pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the federation website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

The federation provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the federation through:

- Ensuring that personal information is not published
- Social media profiles are set to private and not public.
- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk
- Federation staff should ensure that:
- No reference should be made in social media to students / pupils, parents / carers or federation staff
- They do not engage in online discussion on personal matters relating to members of the federation community
- Personal opinions should not be attributed to the federation
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Personal Use:

- Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the federation or impacts on the federation, it must be made clear that the member of staff is not communicating on behalf of the federation with an appropriate disclaimer. Such personal communications are within the scope of this policy
- Personal communications which do not refer to or impact upon the federation are outside the scope of this policy
- Where excessive personal use of social media in federation is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- The federation permits reasonable and appropriate access to private social media sites at the discretion of the Headteacher

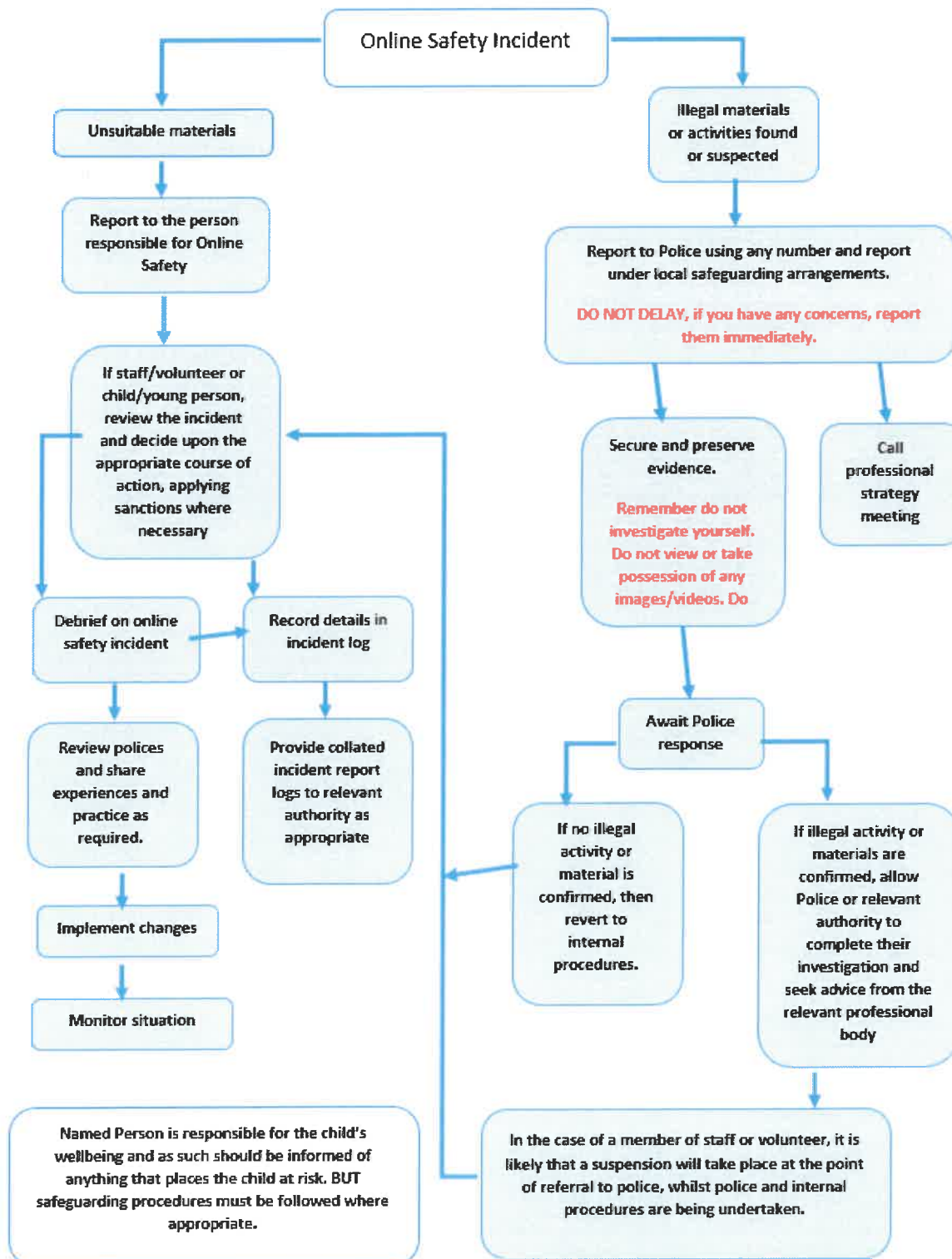
Monitoring of Public Social Media

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the federation
- The federation should effectively respond to social media comments made by others according to a defined policy or process

Responding to incidents of misuse

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart for responding to online safety incidents and report immediately to the police.



Other Incidents

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
 - Internal response or discipline procedures
 - Involvement by the Trust, local authority or national / local organisation (as relevant).
 - Police involvement and/or action
 - If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
 - incidents of 'grooming' behaviour
 - the sending of obscene materials to a child
 - adult material which potentially breaches the Obscene Publications Act
 - criminally racist material
 - promotion of terrorism or extremism
 - other criminal conduct, activity or materials including radicalisation
 - Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

Federation Actions & Sanctions

The federation will need to agree sanctions with the Local Governing Body. The federation will need to deal with incidents as soon as possible in a proportionate manner ensuring that members of the federation community are aware that incidents have been dealt with appropriately. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures.

APPENDIX 1: Staff (and Volunteer) Online safety and ICT Acceptable Use Agreement

Flourish Federation

New technologies have become integral to the lives of children and young people in today's society, both within federation and in their lives outside federation. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate 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 should have an entitlement to safe access to the internet and digital technologies at all times.

This Acceptable Use Policy is intended to ensure:

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

The federation will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for students / pupils learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use federation systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that students / pupils receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the federation will monitor my use of the federation digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, VLE etc.) out of federation, and to the transfer of personal data (digital or paper based) out of federation.
- I understand that the federation digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the federation.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using federation 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 will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the federation's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (eg on the federation website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites in federation in accordance with the federation's policies.
- I will only communicate with students / pupils and parents / carers using official federation 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.
- The federation have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the federation:
- When I use my mobile devices (laptops / tablets / mobile phones / USB devices etc) in federation, I will follow the rules set out in this agreement, in the same way as if I was using federation equipment. I will also follow any additional rules set by the federation about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the federation ICT systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (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 federation 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 try (unless I have permission) to 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 federation policies.
- I will not disable or cause any damage to federation equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others. Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.
- I understand that data protection policy requires that any staff or student / pupil 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 federation 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.

When using the internet in my professional capacity or for federation sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work

- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

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

- I understand that this Acceptable Use Policy applies not only to my work and use of federation digital technology equipment in federation, but also applies to my use of federation systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the federation
- 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 the Local Authority and in the event of illegal activities the involvement of the police.
- I have read and understand the above and agree to use the federation digital technology systems (both in and out of federation) and my own devices (in federation and when carrying out communications related to the federation) within these guidelines.

User Signature

I agree to follow this code of conduct and to support the safe use of ICT throughout the federation.

Full name:(PLEASE PRINT)

Job title:

Signature:

APPENDIX 2: Online safety and ICT Acceptable Use Agreement for Parents/Carers

Parent's/Carer's name: _____ (PLEASE PRINT)

Child's name: _____ **Year and Class:** _____

Child's name: _____ **Year and Class:** _____

As the parent/carer of the above child(ren), I grant permission for my child(ren) to have access to use the Internet, the Virtual Learning Environment, federation email and other ICT facilities at Flourish Federation.

I know that my daughter or son has signed a form to confirm that they will keep to the

federation's rules for responsible ICT use, outlined in the online safety and ICT Acceptable Use Rules for Children. I also understand that my son/daughter may be informed, if the rules have to be changed during the year. I know that the latest copy of the online safety and ICT Acceptable Use Policy and the Rules are available on the Flourish Federation website and that further advice about safe use of the Internet can be found through our links on the website.

I accept that ultimately the federation cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the federation will take every reasonable precaution to keep children safe and to prevent children from accessing inappropriate materials. These steps include using a filtered internet service, secure access to email, employing appropriate teaching practice and teaching online safety skills to children.

I understand that the federation can check my child's computer files, and the Internet sites they visit. I also know that the federation may contact me if there are concerns about my son/daughter's online safety or e-behaviour.

I will support the federation by promoting safe use of the Internet and digital technology at home and will inform the federation if I have any concerns over my child's online safety.

Parent's signature: _____ **Date:** _____