HUNSLEY PRIMARY
inspire·aspire

E–Safety Policy

This policy is applicable to: Hunsley Primary

Intended audience: Staff, Parents, Pupils

Important: This document can only be considered valid when viewed on the school website. If this document has been printed or saved to another location, you must check that the version number on your copy matches that of the document online. **Name and Title of Author:**	Simon Windeler, IT Manager (Adapted by L Hudson and authorised by the Hunsley Primary LGB)
Name of Responsible Committee/Individual:	Hunsley Primary Local Governing Body
Implementation Date:	January 2018
Review Date:	January 2019
Target Audience:	All Staff, Parents, Pupils / Pupils, other stakeholders (e.g. school visitors)

E-Safety Policy

Contents

1. Introduction

Ofsted have defined e-safety thus (in 'Inspecting e-safety in schools' briefings):

- In the context of an inspection, e-safety may be described as the school's ability to protect and educate pupils and staff in their use of technology and to have the appropriate mechanisms to intervene and support any incident where appropriate.

E-safety will be inspected in relation to the following areas:

- The behaviour and safety of pupils at the school.
- The quality of leadership in, and management of, the school

There are three areas of e-safety risk in relation to pupils:

- Being exposed to illegal, inappropriate or harmful material.
- Being subjected to harmful online interaction with other users.
- Personal online behaviour that increases the likelihood of, or causes, harm.

An outstanding school will demonstrate that:

- All groups of pupils feel safe at school and at alternative provision placements at all times. They understand very clearly what constitutes unsafe situations and are highly aware of how to keep themselves and others safe, including in relation to e-safety.

2. Aims

This policy aims to set out the school's position in how it will strive to provide an e-safe environment for all of the school community whilst using ICT within the school, and how it will also strive to ensure that its members also use ICT in a safe and responsible manner whilst outside of the school grounds.

This policy will detail the individual responsibilities of each of the key people in the school and the Trust who have a role to play in fulfilling this policy and its related procedures.

This policy applies to all staff, pupils / pupils, governors and parents of the school community. It should be read in conjunction with the supporting policies and related information that is detailed below.

Hunsley Primary believes that ICT can and should be used to enrich the education of all pupils. ICT also provides the staff of the school with a great many tools to help them play their part in providing the pupils of the school their education. Whilst the school sees the benefits of using this technology, it is also aware of the potential risks that the internet, ICT and related technology can pose. The school believe that e-Safety is the responsibility of the whole school community, and that all members of that community have their own part to play in ensuring that everyone can gain from the benefits that the internet and ICT afford to teaching and learning, whilst remaining safe.

Social Networking is becoming increasingly popular tool within our environment to support learning and encourage creative use of the internet, and to publish and share content. These technologies need to be used in a safe and responsible way, and appropriate online behaviour encouraged.

Although we encourage staff to use social networking (Hunsley Primary Facebook and Twitter) to promote learning within school, we also expect staff to maintain a professional level of conduct in their use of these types of technologies.

3. Content

Risks of ICT Use and the Internet

The school has identified the following risks that ICT and the internet can pose to its community: [1]

- Obsessive use of technologies, the internet and ICT
- Exposure to inappropriate materials
- Inappropriate or illegal behaviour
- Physical danger or sexual abuse
- Being subjected to harmful online interaction with other users.
- Inappropriate or illegal behaviour by school staff

Creating a Safe ICT Learning Environment

The school believes that the best way to provide a safe ICT learning environment is a triple-fold matter:

1. Create an infrastructure of whole school awareness, designated responsibilities, policies and procedures. This can be achieved by:
    - Raising awareness of the risks of technology that is both emerging and already embedded in the school community.
    - Ensuring that the e-Safety policy and education programme adapts to meet these new and emerging technologies and is reviewed as incidents occur.
    - Establishing a clear understanding of the responsibilities of all of those involved with the education of children, with regards to e-Safety.
    - Ensuring that the school's policies and procedures are effective and kept up to date, and also make clear to all members of the school community what is acceptable when using ICT and the internet.
    - Explaining why harmful or abusive images on the Internet might be inappropriate or illegal.
    - Explaining why accessing age inappropriate, explicit, pornographic or otherwise unsuitable or illegal videos is harmful and potentially unsafe.
    - Explaining how accessing and / or sharing other people's personal information or photographs might be inappropriate or illegal.
    - Teaching why certain behaviour on the Internet can pose an unacceptable level of risk, including talking to strangers on social networking; how to spot an unsafe situation before it escalates, and how illegal practices such as grooming can develop.
    - Exploring in depth how cyber bullying occurs, how to avoid it, how to stop it, how to report it and how to deal with the consequences of it.
2. Make use of effective technological tools to ensure the safe use of the internet and school ICT systems. These include:

[1] This list is by no means exhaustive and will have a range of applications for different year groups, but means to highlight some of the main areas of risk that the school has identified and to identify early in the school career the opportunities to protect and educate the children for future use of ICT.

- Firewall protection to the school's network.
- Virus protection of all relevant IT equipment connected to the school's network.
- Filtering, logging and content control of the school's internet connection.
- Monitoring systems.

3. Develop an internet safety education programme for the whole school. This will consist of:
    - An on-going education programme for the pupils at the school, so that they are given the tools to formulate and develop their own parameters of acceptable behaviour and take these with them when they leave the school.
    - Continued Professional Development of all staff to ensure that they are equipped to support the pupils at the school, and are also fully aware of their responsibilities in using ICT, both in and out of the school.
    - An on-going education and information programme for parents, carers and the wider community so that they have the knowledge and tools available to support the actions of the school in these matters.

Head of Hunsley Primary's Responsibilities

1. To take ultimate responsibility for e-safety (with the plan of delegating the day-to-day responsibility to the ESafety Coordinator (ESC) as appropriate, once the school is fully staffed)
2. To ensure that the local governing body is kept informed of the issues and policies.
3. To ensure that the appropriate funding is available to support the technological infrastructure and CPD training for the e-safety programme.

Governing Body's Responsibilities

1. To ensure the designated Safeguarding Governor considers e-safety as a part of the regular review of child protection and safeguarding.
2. To support the headteacher to ensure that the correct policies and procedures are in place, and also that the funding required to achieve these policies and procedures is available.
3. To help in the promotion of e-safety to parents.

E-Safety Coordinator's Responsibilities (when school is fully staffed)

1. To develop and review the appropriate e-safety policies and procedures.
2. To develop management protocols so that any incidents are responded to in a consistent and appropriate manner.
3. To work with the appropriate members of staff to develop a staff CPD programme to cover all areas of e-safety inside and outside of the school environment.
4. To work with the appropriate members of staff to develop an e-safety education programme for the pupils.
5. To work with the appropriate members of staff to develop a parental awareness programme for esafety at home.
6. To maintain a log of all e-safety incidents that occur in the school.
7. To recommend reviews of technological solutions, procedures and policies based upon analysis of logs and emerging trends.

8. To meet with the Designated Safeguarding Officer regularly to discuss e-safety and progress.
9. To liaise with any outside agencies as appropriate.
10. To maintain an appropriate level of professional conduct in their own internet use, both within and outside the school.

Designated Safeguarding Officer's Responsibilities (currently Head teacher)

1. To seek professional development on the safety issues relating to the use of the internet and related technologies, and how these relate to children.
2. To liaise with key school leaders on specific incidents of misuse.
3. Take a proactive role in the e-safety education of the school's pupils.
4. Develop systems and procedures for supporting and referring pupils identified as victims or

   perpetrators of e-safety incidents.
5. To maintain an appropriate level of professional conduct in their own internet use, both within and outside the school.

Trust IT Support Team Responsibilities

1. To perform regular audits and checks of the school's networked systems to look for signs of misuse or inappropriate files. Any such findings would need to be reported to the Head of school and Police if necessary.
2. Review the technological systems upon any discovery or breach of the acceptable use policy, to ensure that the same breach does not happen again.
3. Liaise with the Head if any breach can be traced back to an individual pupil
4. Liaise with the Head if any breach can be traced back to an individual member of staff.
5. Provide the technological infrastructure to support the e-safety policies and procedures.
6. Reporting any network breaches of the school's Acceptable Use Policy or e-safety Policy to the Head
7. To maintain an appropriate level of professional conduct in their own internet use, both within and outside the school.

Teaching Team / Associate Staff Team Responsibilities

1. To develop / deliver schemes of learning to ensure that e-safety is embedded in their areas teaching practice.
2. To maintain an appropriate level of professional conduct in their own internet use, both within and outside the school.
3. To develop and maintain their own knowledge of internet safety issues.
4. To ensure that any incidents of ICT misuse are dealt with through the correct channels, in line with the ICT and e-Safety policies.
5. To ensure that any pupils who experience problems when using the internet are appropriately supported

6. To develop and maintain a knowledge of e-safety issues, with particular regard to how they might affect children.
7. To implement school e-safety policies through effective classroom practice.
8. To ensure any incidents of ICT misuse are reported through the correct channels.
9. To ensure that the necessary support is provided to pupils who experience problems when using the internet, and that issues are correctly reported to the Head teacher or appropriate school leader
10. To plan classroom use of ICT facilities so that e-safety is not compromised.

Special Educational Needs Coordinator Responsibilities

1. To develop and maintain a knowledge of e-safety issues, with particular regard as to how they may affect children.
2. To develop and maintain additional policies and e-safety materials in conjunction with key staff, tailored to meet the needs of SEN pupils
3. To liaise with parents and carers of SEN pupils to raise awareness of the school's e-safety position and how the parents can support the school's position.
4. To maintain an appropriate level of professional conduct in their own internet use, both within and outside the school.

Pupil Responsibilities

1. To uphold all school e-safety and ICT policies.
2. To report any misuse of ICT within the school to a member of staff.
3. To seek help or advice from a teacher or trusted adult if they or another pupil experience problems online.
4. To communicate with their parents or carers about e-safety issues and to uphold any rules regarding esafety that may exist in the home.

Parents' and Carers' Responsibilities

1. To help and support the school in promoting e-safety
2. To discuss e-safety concerns with children and to show an interest in how they use technology.
3. To take responsibility for learning about new technologies and the risks they could pose.
4. To model safe and responsible behaviour in their own use of the internet.
5. To discuss any concerns they may have about their children's use of the internet and technology with the school.

4. Supporting Policies and Related Information

South Hunsley School and Sixth Form College / Hunsley Primary/Education Alliance supporting policies:

- Safeguarding Policy
- Expectations and Code of Conduct for Staff
- Prevent Policy
- Behaviour for Learning Policy
- PSHE Policy

5. Procedure for Policy Implementation

The procedural documents for this policy are attached as an appendix.

- Appendix 1 – Procedure for Implementation
- Appendix 2 – e-Safety Incident Reporting Flowchart

e-Safety Policy Appendix 1 - Procedure for Implementation

The Head of Hunsley Primary will ensure that all staff are aware of the policies and procedures being implemented to meet the e-Safety remit. There will be information available to all staff about the technologies that are already in use at the school as well as new and emerging technologies that they may come across in their professional practice. All staff will be given the opportunity to feedback into the school's e-Safety discussions, be given clear guidance to what the procedures are and know who they should speak to regarding any issues.

In the first instance, all staff will receive a basic introduction into the e-Safety programme at the school, and be directed towards the resources that have been made available.

An area of the W-Drive contains relevant resources and links to information regarding the safe use of new technologies within a school environment. Displayed around school is documentation of all people’s roles with regards safeguarding in the school.

The Headteacher will work with the HR Team to ensure that the school's induction and CPD programmes include adequate provision for the delivery of e-Safety training.

E-Safety will form a part of the Child Protection Induction for new staff starters and direct them towards the existing policies, procedures, resources and course of action.

Pupils

The pupils at the school will be made aware that there is a whole school approach to e-Safety (Hunsley Primary Safe APPS) and their roles and responsibilities within this e-Safe environment will be made clear to them. Pupils will be invited to participate in the future planning and discussions regarding e-Safety and their opinions will be gauged as to the effectiveness of the provision.

Through assemblies and the PSHE programme, pupils will be made aware of policies and methods of enforcing these policies.

Parents and Carers

The parents and carers of the school will be made aware of policies and procedures and how they can help in ensuring that Hunsley Primary is an e-Safe school. We will ensure that parents and carers can access information regarding the risks of new technologies, but also how they can ensure these technologies are being used safely.

An area on the School's Website contains useful links and information for parents and carers regarding e-safety. This area will also contain links to the school's e-Safety policy and the Safeguarding Policy.

ParentLearn workshops will be delivered to give parents the opportunity to understand e-safety topics and new risks children are opposed to.

Firewall

The school has a perimeter firewall, which is supplied by Smoothwall. This physical hardware device sits at the edge of the network and allows only specific traffic in and out of the network. All intrusion attempts from both sides of the network can be logged and analysed for security audits.

The responsibility lies with the Trust IT Support Team for ensuring that the firewall is correctly configured and that intrusion logs are regularly checked.

Anti-Virus Protection

The school has purchased an Enterprise License for Microsoft’s Endpoint Protection. This anti-virus software is installed on all Microsoft Windows based servers and computers on the school network.

It is the responsibility of the Trust IT Support Team to ensure that all necessary computers on the school network are running current anti-virus software and that regular scans are performed. If a virus out-break happens, the Trust IT support team must notify the Head of Hunsley Primary and as soon as possible isolate the infection.

Any devices being brought into to school and connected to the school's ICT network must be proven to have up-to-date Anti-Virus protection and be cleared by the Trust IT support team before being connected.

Filtering and Logging of Internet Access

The school has a web caching and proxy server that contains accredited filter lists. This enables the school to log all Internet traffic in the school and allow different sites to different groups of users. This server ensures that all internet use on the school's network is logged to an individual user of the network. If the device being used to access the Internet is not a school owned device, the user will have to present valid school network credentials before they can gain any access to the school's Internet connection. If an e-safety incident requires it, all Internet access logs of any pupil or staff member can be retrieved to support any required processes.

It is the responsibility of the Trust IT support team to ensure that all computers connected to the school's network only receive an Internet connection by going through the proxy server. The Trust IT support team, on request, will add any sites that have been discovered through e-safety incidents to the block lists of the filtering server. The Trust IT support team will perform regular reports from the logs of the web proxy server to present at the e-safety management group, with regards to the most accessed sites and most active Internet users in the school.

Monitoring Systems

The school has many different monitoring system at its disposal;

- All files stored on the school's servers can be searched and checked
- Every single action performed on the network is logged against the user that performed the action. These logs can be accessed to provide evidence for an e-safety incident
- All computer use is monitored centrally against a set of predefined word lists and use or viewing of inappropriate text is logged with a screen grab and the details of the offence, user and time it occurred
- Any incident that has a sanction attached to can be entered into the school's MIS system under e-safety

E-Safety Education

Pupils

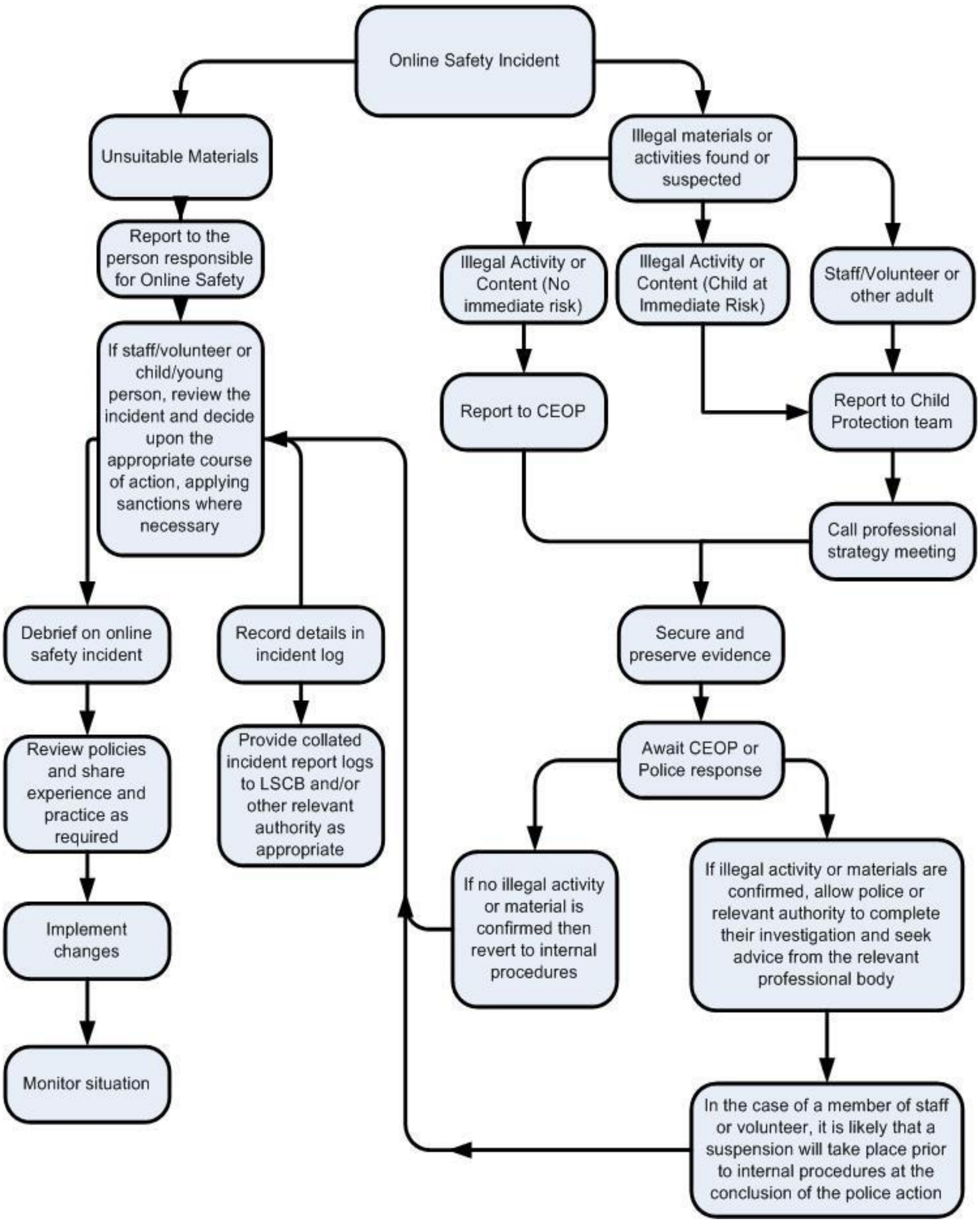
All pupils at the school will receive an on-going, age-appropriate e-Safety education programme.

This programme will inform the pupils of the issues and potential risks of using the internet and emerging technologies. It will also equip them with the knowledge to ensure they are adequately protected and informed when in these environments. They will be given the information required to know who they can talk to and what their rights are if they do experience issues whilst using the internet.

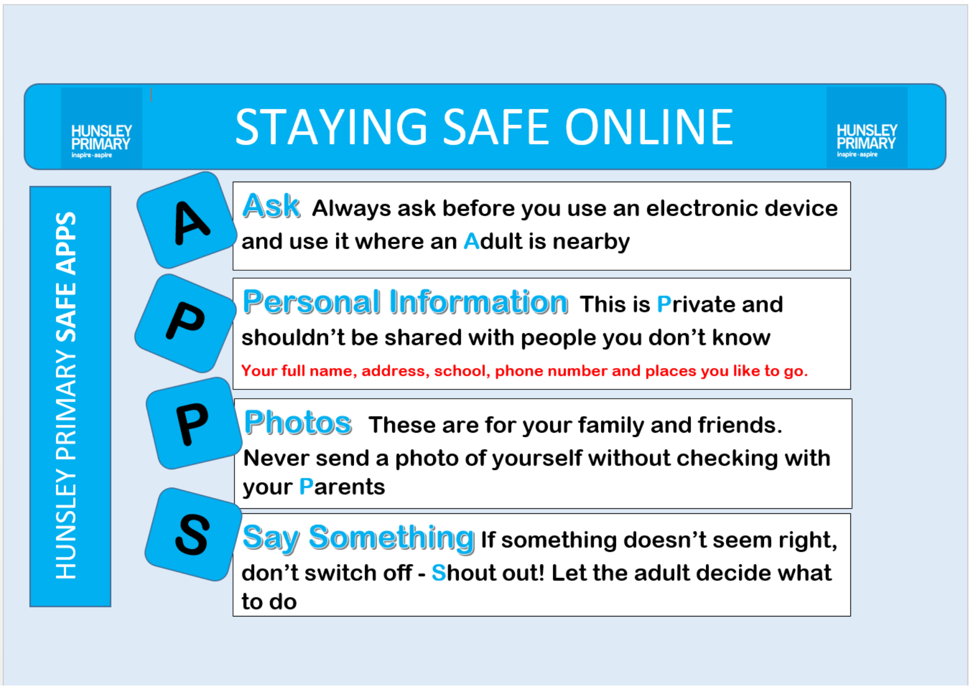
PSHE, Computing and Personal Development week curricula will be regularly reviewed to ensure that e-Safety is incorporated into its programme.

The SENCO will work with the Head of School or other appropriate leaders to ensure that there are accessible and adequate resources available for the SEN pupils / pupils of the school to receive the same e-Safety education as the rest of the school.

Responding to incidents of misuse – flow chart Appendix 2


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

Hunsley Primary Safe APPS



HUNSLEY PRIMARY inspire · aspire
HUNSLEY PRIMARY inspire · aspire
HUNSLEY PRIMARY SAFE APPS
A
P
P
S

STAYING SAFE ONLINE

Ask Always ask before you use an electronic device and use it where an **A**dult is nearby

Personal Information This is **P**rivate and shouldn't be shared with people you don't know

Your full name, address, school, phone number and places you like to go.

Photos These are for your family and friends. Never send a photo of yourself without checking with your **P**arents

Say Something If something doesn't seem right, don't switch off - **S**hout out! Let the adult decide what to do

Hunsley Primary Statement for the Safe Use of Media

Use of Social Media

Facebook, twitter and Hunsley Primary website

- All images used for social media content will be drawn solely from pupils whose parents / carers have given explicit permission to do so
- All images posted will be checked against the permissions list prior to uploading, every time the process is carried out.
- All images of parents, visitors and other members of the public will only be used outside of school once written permission has been acquired.
- If in any doubt, a further check and consent will be sought, and if in continued doubt the images will not be used.
- Verbal consent is not sufficient; consent must be given in writing (email is acceptable)
- Each year, the Data Information form will be revised to ensure that all data required for Multi Media applications will be updated where necessary
- Images will only be posted by designated staff – school / Trust administrators / Head of School

Use of iPads and cameras in the classroom

For assessment and evidence capture

- Only school iPads will be used to capture evidence (video, audio and photographs)
- Images will only be stored on the iPad photo reel and then moved promptly to the secure W Drive folder for photographs
- All remaining photographs and video will be permanently deleted, firstly from the photo reel and secondly from the 'Recently Deleted' folder
- Staff, volunteers and visitors will not use personal devices for image capture at any time
- Staff personal devices (e.g. Phones) will remain in the Main Office area at all times during the school day
- All iPads will be kept in school and secured, using the lockable unit
- The school camera may be used for the same purpose and will not be taken out of school, unless under the agreement of the Head of School for educational visits, sports event and other external events where evidence might be captured
- Staff working on evidence folders at home will only do so via the secure 'Remote Desktop', password protected websites and the W-Drive folders.
- Multi Media files will not be stored in any other device or space than in the two above spaces (iPad Photo Reel – temporary storage- and the W-Drive – permanent storage)
- Images stored online in the Tapestry folders are stored securely via the password protected portal and are not subject to public access.
- Print images will be used in the classroom for display and training purposes, unless parents request not to

Use of images in Learning Journey documents

For sharing with parents, carers and Local Authority

- Permissions will be sought from parents and carers to share images in print form only, for example in group shots. Images will never be used where permission is not given