FERNDOWN UPPER SCHOOL

Online and Digital Technology Policy

Combining all online and digital policies

Policy First Adopted September 2019

To be reviewed every July.

Reviewed	September 2019
Reviewed	July 2020
Reviewed	Changes July 2021
Reviewed	July 2022
Reviewed	July 2023
Reviewed	August 2024
Reviewed	September 2025

This policy links to many other school policies including Data Protection, Risk Management, Accessibility, Student Behaviour, Code of Conduct and Child Protection.

Contents

Introduction

The use of Information Technology at Ferndown Upper School is viewed as an essential resource for all pupils, staff, volunteers, governors and visitors/guests and the School is constantly looking at ways to improve and develop *ICT* (Information Communication Technology).

New technologies have become integral to the lives of children and young people in today's society, both within Schools and in their lives outside of School.
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 Internet access at all times.

This policy is intended to address both School owned computer hardware in addition to the use of non-School owned electronic devices by pupils, staff, volunteers, governors and visitors/guests at Ferndown Upper School. These include smart phones, tablets, laptops, wearable technology and other devices used to access the Internet and/or store school information as well as users' own data. This is commonly referred to as 'Bring Your Own Device' (BYOD). The School recognises that mobile technology offers valuable benefits to pupils from a teaching and learning perspective. Our School embraces this technology but requires that it is used in an acceptable and responsible way.

This policy covers the use of such devices and the liability of the School for mobile devices used on School premises. The use of such devices on School grounds is at the discretion of the School. Pupils and staff at the School can be granted the right to use their mobile devices provided that they adhere to this ICT Acceptable Use Policy (ICT AUP) together with any associated polices and accept the agreement and guidelines set out herewith.

1. Requirements for Online and Digital Technology Use in Schools

1.1 Department for Education (DfE)

Taken from: Keeping Children safe in Education: Statutory Guidance for Schools and Colleges

Online safety

It is essential that children are safeguarded from potentially harmful and inappropriate online material. An effective whole school and college approach to online safety empowers a school or college to protect and educate pupils, students, and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate.
As such, governing bodies and proprietors should ensure appropriate filters and appropriate monitoring systems are in place. Additional information to support governing bodies and proprietors keep their children safe online (including when they are online at home) is in KCSIE. https://www.gov.uk/government/publications/keeping-children-safe-in-education--2

1.2 Dorset Council

Dorset council have a dedicated team to support e-safety in schools, their dedicated website is found here: https://www.dorset.police.uk/help-advice-crime-prevention/scams-fraud-cyber-crime/cyber-crime/

The Safer Schools Team are always available for general queries regarding Online Safety of Staff and Students. For safeguarding or immediate concerns the safeguarding lead, Headteacher or Online Safety Officer must be contacted as soon as possible.

1.3 Online Safety and Digital Working Group

1.3.1 Premise

With digital technology becoming a more integral part of the workplace and education, Ferndown Upper School is aiming to become a leader in Online Safeguarding and Safety Awareness. To do so this will be managed and driven by an Online Safety and Digital Working Group. We aim to achieve the official online safety mark by the end of the academic year.

1.3.2 Responsibilities

- To ensure a clear Online Safety and Digital Technology Policy is implemented to enable safeguarding of staff and students from online threats.
- The group will meet half-termly to discuss issues surrounding cyber-safety and digital technology use in school.
- To be active in communicating to students safe practice in using digital technology inside and outside of school.
- To keep parents and carers updated and informed about e-safety issues that may affect them or their children.
- To keep staff and governors updated on e-safety issues and ensure *CPD* (Continuing Professional Development) is provided where applicable on aspects of safeguarding and technology use.

- To continually evaluate the Online Safety and Digital Technology Policy to ensure it is up to date with legislation, statutory requirements and adapted where improvements can be made.

1.3.3 Members

The group requires representation from all school stakeholders.

The Digital Management Group

Online Safety Lead
The Online Safety Officer is the designated lead in all aspects of online and digital technology use in school, including the management of the whole-school policy. They also chair the Digital Community Group.

Data Protection Officer
The designated Data Officer of the school is closely linked to aspects of the policies associated with the Digital Working Group and will be required to attend some Digital Management Group meetings.

Safeguarding Team
At all meetings a designated member of the safeguarding team must be present. This could be the Online Safety Officer or any other Safeguarding team member.

IT Technical Support
IT Technical team member should be present to update on common issues, software and hardware updates affecting safeguarding and technology use.

Governor
A representative of the governing body should either be present at the meeting or updated on issues surrounding this policy after each meeting of the working group.

The Digital Community Group (meets twice a year)

Parents and Carers & Students

2. Digital Awareness and Education

In a world with increased digital and online content it is imperative that all stakeholders in schools, particularly young people are made aware of developments in this area. This includes e-safety, cyber security and the development of critical thinking skills that help them make better factually informed choices in their future lives.

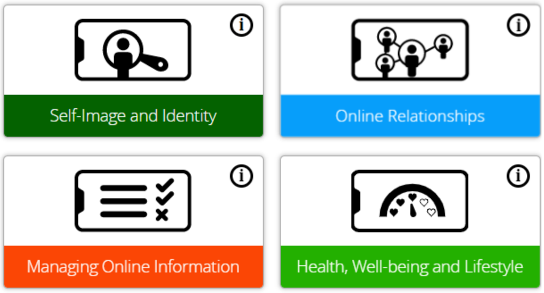
Ferndown Upper School has developed an extensive programme of Digital Awareness and Education to improve safeguarding of staff and students and make the best use of digital technology.

2.1 Digital Literacy

Digital literacy is an essential aspects of everyday life and in the workplace.

2.1.1 CREATE EFFECTIVE DIGITAL CITIZENS |

Digital Citizenships is a major strand of the PSHE and Safeguarding curriculum by supporting Digital Citizenship and Online Safety. We follow the SWGFL curriculum and have 8 main themes in the curriculum which is delivered in a variety of ways. These also fully cover the '4Cs' categories of risk explained in section 8.1.



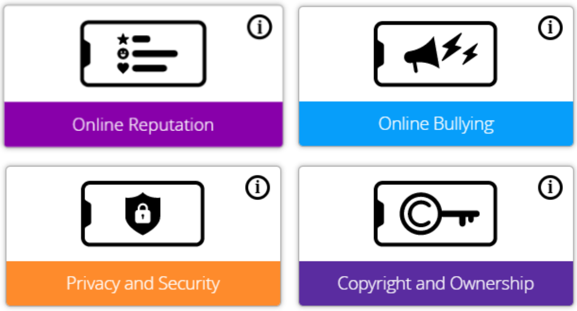
- Year 9 – PSHE Curriculum
- Year 10-13 – Drop Down sessions
- Tutor Group Inputs

- Computing Lessons (Y9-13)

The structure of topics in digital drop down sessions (and Year 9 PSHE) are outlined in the table.

We also promote internet safety week and contribute towards anti-bullying week as Online Relationships is now a major component of this curriculum (including RSE).

To support the delivery of these elements of the curriculum we will be using the ‘Project EVOLVE’, which is library/toolkit of assessment and resources that can be used to track our students engagement with this part of the curriculum.



Medium Term Plan for Digital Citizenship Curriculum

Session Number	Year 9	Year 10	Year 11	Year 12	Year 13
Session 1 **Healthy Device use**	Technology Addiction, Addictive Design vs Humane Design, Healthy Digital Habits	Media Balance, Positive and Negative impacts of digital media, improving digital well-being	Difference between active and passive use. How social media makes people feel. Actions to increase positive social media outcomes.	Addiction, humane design, device use, device addiction	Health effects of screen time, passive and active use, media balance
Session 2 **Digital Privacy**	Privacy, Privacy Settings	Cookies, GDPR, online tracking, targeted advertising, personal data use	Emerging risks to privacy, facial recognition, weighing risk/benefits	Personal information, data collection of minors, social media consent, age debate	Surveillance, Privacy, Social Media in schools, free speech, government tracking
Session 3 **Digital Footprint**	Digital Footprint, Oversharing, Social Media Use, Online Relationships	Digital Footprint, Digital Reputation, Sharenting, Child Protection	Curated self vs real self, avatars, risks	Digital Footprint, personal branding, hurting future opportunities	Digital footprint, using social media to showcase success
Session 4 **Online Relationships**	Online Relationships, Sexting, Self-Disclosure, Red-Flag Feelings	Grooming, Red-Flag Feeling, Online Relationships, Online Risk	Online relationships, How devices affect relationships, healthy vs unhealthy relationships, strategies to navigate challenging relationships	Code-switching (changing language, behaviour/appearance based on who you're with or where you are), collaboration	Civil discourse, debating in online environments, uncivil online discourse
Session 5 **Cyberbullying/Hate-Speech**	Cyberbullying, Hate Speech, Homophobia	Cyber Bullying, Digital Dilemmas (How to deal with embarrassing situations that may arise)	Counter speech, hate speech, extremism, xenophobia	Online disinhibition effect, cyberbullying, online anonymity	Freedom of speech, hate speech, prejudice
Session 6 **Media Literacy/**	Media Literacy, Bias, News Cycle	Fake News, Disinformation, lateral reading,	Confirmation bias, cognitive	Advertisement, marketing,	Filter bubbles, personalised content,

Online Citizenship		misinformation, corroboration	bias, fake news, misinformation	clickbait, disinformation	disinformation, bias

2.2 For Students

All Students

A general but vital focus of the school is to develop independent learners.

The use of Bromcom and curriculum learning packages are bought by the school to develop independent learner via the use of Digital Technology.

Year 9

All Year 9s study computing, PSHE and tutor group activities.

Year 9-13 Drop Down Sessions

Year 9-13 have ‘drop down’ sessions. Where the Safer Schools Team deliver a talk on Online Safety and the law and two lessons are delivered on Cyberbullying and Cybersecurity.

2.3 For Parents

To involve more parents in Digital Literacy education there are a number of ways connections are made to parents.

Year 9 Induction: Parents have input by the Online Safety Lead regarding e-Safety and role of the parent in this.

Digital Community Group: Parents are invited to the group to discuss issues surrounding e-safety in and out of school.

Half-termly e-Safety Newsletter: From the *SSCT* (Safe Schools & Communities Team) newsletter.

2.4 For Staff

Online Safety: CPD annually is used to train staff in strands c, d and f in digital literacy, cyber security, filtering and monitoring, AI and in the safeguarding of students.

3. Digital Devices and Acceptable Use Policy – split staff and students

Ferndown provides a range of digital facilities for both staff and students. This includes the 'Bring Your Own Device' policy for staff and students. The policies below aim to minimise hardware and software damage to IT systems at the school. By doing this safeguarding of staff and students is most effective and costs are kept to a minimum.

This Acceptable Use Policy is applicable to all members of the school community, whether working from school or from home and is intended to ensure that:

All users will act responsibly and stay safe while using the Internet, School network and other communication technologies whether they are working at school or at home.

- School ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and other users at risk.
- Users are protected from potential risk in the use of ICT in their everyday work.
- Clear guidance on how to minimise risks and how to deal with any infringements are provided.

The School will try to ensure that pupils, staff, volunteers, governors, and visitor/guest users will have adequate access to ICT to enhance their work or learning opportunities for pupils (where applicable) and will, in return, expect all users to agree to be responsible users.

Device Types:
For the purpose of this acceptance policy, the word 'device' means a privately owned or School-owned wireless and/or portable electronic piece of equipment that includes laptops, netbooks, smart phones, wearable technology, tablets/iPads or slates.

The word 'user' refers to any individual either connecting to the School hard wired network or wireless networks. For example: pupils, staff, volunteers, governors, visitors/guests.

3.1 Acceptable Use Policy Agreement

3.1.1 All users must familiarise themselves and follow the guidance, it is mandatory.

3.1.2 Pupils, staff, volunteers, governors and visitor/guest users should understand that they must use School ICT systems in a responsible way, to ensure that there is no risk to their safety or to the safety and security of the ICT systems and other users. This is applicable when working in school or at home.

3.1.3 When users use their own personal mobile devices (tablet devices, laptops, mobile phones, USB devices, etc.) in School, they will follow the rules set out in this agreement in this policy, in the same way as if they were using School equipment. They will also follow any additional rules set by the School about such use and ensure that any such devices are protected by up to date anti-virus software and are free from viruses.

3.1.4 Networked computers will gain access through the School's firewall, which is maintained by the ICT Support. However no firewall is considered to be impenetrable so additional security products will be used in conjunction with the firewall. However, all School users are expected to maintain a level of 'personal responsibility' when using our system and any mobile technologies onsite and access via any illicit means to undesirable websites will be treated as a threat to our community and system integrity and users may be disciplined accordingly.

3.1.5 School devices are for members of staff use only and should not be used by non-staff members e.g. family. We advise that school devices are for school use only, not personal use.

3.2 School Internet and E-mail Systems

3.2.1 Ferndown Upper School will provide a filtered educational internet and email service which is monitored in School and by our provider to reduce the risk of access to inappropriate material.

3.2.3 All users must be aware that some services available on the Internet may be offensive. Whilst the School takes reasonable and necessary precautions, including filtering and other security measures, to help ensure a safe computing environment for all users, the School cannot make an absolute guarantee that a user will not be able to access relatively inappropriate material, and the School cannot be held responsible for the voluntary actions of the users in this regard.

3.2.4 The School will not be responsible for any content accessed by a user using their own devices through non-school controlled wireless or network systems, such as personal 3G and 4G networks, 'Hotspots', Proxy or VPN bypass Systems.

3.2.5 The School accepts no responsibility for information or material contained on any websites; other than its own.

3.2.6 Ferndown Upper School's e-mail and Internet facilities are primarily provided to its users for School related teaching and learning or business purposes only. Any use of the systems for personal or recreational purposes should be within the policies and rules set down by the School, as follows:

3.2.6.1 Personal use of the Internet must not interfere with a user's work commitments (or those of others). If it is discovered that personal usage has been excessive, disciplinary action may be taken and access to the facilities may be withdrawn without notice. The School reserves the right to undertake random checks of users' Internet and email usage.

3.2.6.2 Users are not permitted to enter into any contract or subscription on the internet on behalf of the School, without specific permission to do so.

3.2.6.3 E-mail should be treated in the same way as any other form of written communication. Users should not include anything in an e-mail which is not appropriate to be published generally. They should exercise care when copying or forwarding e-mails as this may disclose sensitive or confidential information to the wrong person.

3.2.6.4 An email message which is abusive, discriminatory on ground of sex, marital or civil partnership status, age, race, disability, sexual orientation including being or becoming a transsexual person, pregnancy and maternity or religious belief (or otherwise contrary to our Equal Opportunities policy) or defamatory is not permitted.

3.2.6.5 Personal emails must not be accessed on any School equipment.

3.2.6.6 Staff should also refer to guidance set out within the Email Protocol & Guidance and Staff Code of Conduct Policy.

3.2.7 The School can monitor users' Internet, email and network activity; without consent in the following circumstances (in accordance with the Telecommunications [Lawful Business Practice] [Interception of Communications] Regulations 2000): to ensure compliance with regulatory practices; to ensure standards of service are maintained; to prevent or detect crime; to protect the communication system (including unauthorised use and risk of viruses).

3.2.9 Care should be taken when opening files or e-mail attachments received via the Internet or web-based e-mail providers. If there is any doubt or concerns regarding the contents, then please delete the files. If you have any concerns, you should contact the ICT Services/Support Department as soon as possible.

3.2.10 Information received from the Internet should not be uncompressed or executed unless the source is trusted. Under no circumstances should unsolicited data or files be opened, uncompressed or executed.

3.2.11 Users are not permitted to intercept or view an e-mail message or attachments that was originally destined for someone else.

3.2.12 Users must not impersonate another person in a malicious context irrespective of how the logon details to that account were obtained.

3.2.13 If users open inappropriate material this must be reported immediately to the DSL, Online Safety Lead or IT Support.

3.3 School’s Network

3.3.1 Password Security

3.3.1 All access to the network in School will be supervised and available only to those who possess a valid network username and password. Users should be reminded of the need for password security. Students will write passwords down / store it in their phone initially to support remembering them, but after that they are encouraged not to write it down or store a password where it is possible that someone may steal it.
FUS requires that users passwords must meet the following criteria:

- Be at least six characters in length
- Contain at least one uppercase character
- Contain at least one lowercase character
- Contain at least one number
- Contain at least one special character such as a $ or !

Staff passwords are automatically required to be changed every six months, users will be prompted to do so

3.3.1.2 Not use your School network password for any External websites and services that are not synced and managed by IT Support that are work/School related and use your School email address. The password used must be a different password to the one you use on the network.

3.3.2 Personal devices must NOT be plugged into the School’s local area wired network via an Ethernet cable or connected to the School network without approval from the ICT Services & Innovations Manager. Only personal wireless devices may be utilised, through the School’s ‘Student’, ‘Sixth Form’, ‘Staff’ (for pupils and staff) or ‘Guest’ (for volunteers and visitors/guests) wireless networks.

3.3.3 Physical Vandalism is prohibited. Examples of physical vandalism include, but are not limited to the following examples: disconnecting wires on the back of the computer, tearing off labels and other attachments, carving or marking anything onto computer hardware.

3.3.4 Electronic Vandalism is prohibited. Examples of electronic vandalism include, but are not limited to the following examples: opening/changing/deleting files, changing desktop patterns or sound.

3.3.5 Licensing of software is for Ferndown Upper School use only; and not the individual user (unless specifically instructed).

3.3.6 Users should not attempt to compromise the security of the School's network. Examples of this include, but are not limited to: unauthorised access (hacking) into School technical hardware, i.e. servers, network switches, printers, etc; therefore adhering to the Computer Misuse Act 1990.

3.4 Data Encryption, Data Security and Data Storage

3.4.1 Staff and pupils are permitted and encouraged to store or save their data onto the School's secure central server, shared Microsoft Office 365 area or, where available, within their School Microsoft Office 365 personal online account.

3.4.2 Where possible portable storage devices such as USB data sticks will be encrypted before use with individual passwords. The School will enforce the encryption of USB portable storage devices when accessed on the School network. Users are encouraged however not to store any sensitive or personal data on any portable devices

3.4.3 The School aims to replace any devices which cannot be encrypted and which are capable of storing personal data where it is possible to do so.

3.4.4 Users will not publish any documents containing personal data or critical information on externally accessible websites, unless remote (Internet) access to this data is configured to require user authentication.

3.4.5 The School takes its compliance with the General Data Protection Regulation (GDPR) seriously and aims at all times to keep personal data secure. It takes suitable measures to prevent unauthorised or unlawful processing of personal data and accidental loss or destruction of or damage to personal data. All members of School Staff and Governors are required to undertake GDPR training. The training provided is designed to help Staff understand key areas of compliance and also to provide evidence that staff have read and understood relevant policies and documents.

3.4.6 All incidents resulting in a breach of these guidelines must be reported to the School's Data Protection Officer

3.4.7 Staff

3.4.7.1 Staff will only transport, hold, disclose or share personal information about themselves or others, as outlined in the Data Protection Regulation (GDPR) Policy.

3.4.7.2 Staff will not be permitted to remove or copy sensitive or personal digital data from School network unless the data storage device is encrypted and is transported securely for storage in a secure location.

3.4.7.3 Paper based protected and restricted data must be held in lockable storage. Staff should think before they leave data unattended.

3.4.7.4 Staff should understand that General Data Protection Regulation Policy requires that any staff or pupil data to which they have access, will be kept private and confidential, except when it is deemed necessary that they are required by law or by School/Trust policy to disclose such information to an appropriate authority.

3.4.7.5 If staff are looking to purchase or use any online IT systems or services that store or process pupil or parent personal data they should in the first instance liaise with the ICT Services and Innovations Manager in order for a GDPR Data Audit and Data Protection Impact Assessment to be undertaken.

3.4.7.6 The Data Controller (Director of Operations) in the School is responsible for ensuring that personal data stored on School systems regarding staff, pupils and parents is appropriately restricted and only accessible to designated individuals. Staff are strictly prohibited from storing pupil or parent data on their own personal devices. Staff are therefore expected to act responsibly if using their personal mobile device for School business. They must delete sensitive or commercial emails from their device once the task has been completed and also delete any attachments to emails e.g. data sets/spreadsheets once finished.

3.4.7.7 Staff should also refer to guidance set out within the Email Protocol and Guidance Document and Staff Code of Conduct Policy

4 Appropriate use of Social Networking/Media Sites, AI and Online Safety – need to split into different sections and user sections

Social media is a fun part of everyday life, but it can carry risks. The following bullet points are intended to help pupils and staff avoid any pitfalls, while still making best use of social media for teaching/learning and research as well as social purposes.

'A social networking site is any website which enables its users to create profiles, form relationships and share information with other users. It also includes sites which have online discussion forums, chat-rooms, media posting sites, blogs and any other social space online. They include, but is not limited to sites such as Facebook, Pinterest, Bebo, Tumblr, LinkedIn, Twitter, MySpace, Ping, Wikipedia, Google Plus+, LiveJournal and even YouTube.'

AI as an emerging technology e.g. ChatGPT – use of this in school and for school work may constitute cheating – students should not use this to produce work – unless specified in the brief to do so.
The School reserves the right to use AI detection software for any work submitted – with a particular focus on submitted coursework to meet exam board requirements.

4.1 Students

4.1.1 Pupils should familiarise themselves and follow the guidance as outlined in this Online Safety Policy.

4.1.2 Pupils must not use any social network site to attack, abuse or bully any School staff, other pupils or people. Pupils must not use school systems, including Teams for personal communication or posting inappropriate images / messages. School systems should be used for work related content only.

4.1.3 Pupils must not include contact details or pictures, etc. of other pupils or members of staff without their prior permission.

4.1.4 Pupils are strongly advised to not use any social networking site or pages in any way that may compromise current or future education at the School. Students on placements using professional platforms like LinkedIn must have staff permission from their placement to link to them and ensure appropriate behaviour on the sites.

4.1.5 Pupils should never reveal confidential information about the School or its staff or pupils.

4.1.6 Pupils should take effective precautions when using social networking sites to ensure their own personal safety and to protect against identity theft.

4.1.7 Pupils need to be aware that most pupils are minors (under the age of 18 years of age) and that any interactions with them should not only be approached with some caution, but also that the content of conversations/responses is suitable for members of this age group.

4.1.8 Pupils need to consider intellectual property rights, copyright and ownership of data when using social media.

4.1.9 Individuals should exercise caution when interacting with, and responding to, potentially contentious posts on social media sites.

4.1.10 Students should not use AI for school work, unless the brief says to – this could constitute cheating.

4.2 Staff

4.2.1 Objectives

4.2.1.1 This policy sets out Ferndown Upper School policy on social networking. New technologies are an integral part of our lives and are powerful tools which open up teaching and learning opportunities for schools' staff in many ways. This document sets out Ferndown Upper School policy on social networking and aims to:

- Assist schools' staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice
- Set clear expectations of behaviour and/or codes of practice relevant to social networking for educational, personal or recreational use
- Give a clear message that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken
- Support safer working practice
- Minimise the risk of misplaced or malicious allegations made against adults who work with pupils
- Reduce the incidence of positions of trust being abused or misused

4.2.1.2 Whilst every attempt has been made to cover a wide range of situations, it is recognised that this policy cannot cover all eventualities. There may be times when professional judgements are made in situations not covered by this document, or which directly contravene the standards outlined in this document. It is expected that in these circumstances staff in schools will always advise their head teachers of the justification for any such action already taken or proposed. Headteachers will in turn seek advice from the Schools' HR team where appropriate.

4.2.1.3 This policy takes account of employment legislation and best practice guidelines in relation to social networking in addition to the legal obligations of governing bodies and the relevant legislation listed at appendix A.

4.2.1.4 This policy has been agreed following consultation with the recognised trade unions and professional associations.

4.3 Overview and expectations

4.3.1.1 All adults working with pupils have a responsibility to maintain public confidence in their ability to safeguard the welfare and best interests of pupils. It is therefore expected that they will adopt high standards of personal conduct in order to maintain the confidence and respect of their colleagues, pupils or students, public in general and all those with whom they work in line with the school's code of conduct. Adults in contact with pupils should therefore understand and be aware that safe practice also involves using judgement and integrity about behaviours in places other than the work setting.

4.3.1.2 School staff should always maintain appropriate professional boundaries and avoid behaviour, during their use of the internet and other communication technologies, which might be misinterpreted by others. They should report and record any incident with this potential.

4.3.1.3 All staff, particularly new staff, should review their social networking sites when they join the school to ensure that information available publicly about them is accurate and appropriate. This includes any photographs that may cause embarrassment to themselves and the school if they are published outside of the site.

4.3.1.4 Staff should never 'friend' a pupil at the school where they are working onto their social networking site.

4.3.1.5 Staff should never use or access social networking sites of pupils and should never accept an invitation to 'friend' a pupil.

4.3.1.6 Confidentiality needs to be considered at all times. Social networking sites have the potential to discuss inappropriate information and employees need to ensure that they do not put any confidential information on their site about themselves, their employer, their colleagues, pupils or members of the public.

4.3.1.7 Employees need to ensure that when they are communicating about others, even outside of work, that they give due regard to the potential for defamation of character. Making allegations on social networking sites (even in their own time and in their own homes) about other employees, pupils or other individuals connected with the school, or another school, or Dorset County Council could result in formal action being taken against them.

4.3.1.8 Staff are also reminded that they must comply with the requirements of equalities legislation in their on-line communications.

4.3.1.9 Staff must never post derogatory remarks or offensive comments on-line or engage in on-line activities which may bring the school or Dorset County Council into disrepute.

4.4 Communication between pupils / schools staff

4.4.1 Communication between pupils and staff, by whatever method, should take place within clear and explicit professional boundaries.

4.4.2 This includes the wider use of technology such as mobile phones, text messaging, e-mails, digital cameras, videos, web-cams, websites and blogs.

4.4.3 It is the expectation that the school should provide a work mobile and e-mail address for communication between staff and pupils. Staff should not give their personal mobile numbers or personal e-mail addresses to pupils or parents.

4.4.4 Staff should not request, or respond to, any personal information from a pupil, other than that which might be appropriate as part of their professional role.

4.4.5 Staff should ensure that all communications are transparent and open to scrutiny. They should also be circumspect in their communications with pupils so as to avoid any possible misinterpretation of their motives or any behaviour which could be construed as 'grooming' in the context of sexual offending.

4.4.6 Staff should not give their personal contact details to pupils including e-mail, home or mobile telephone numbers, unless the need to do so is agreed with senior management and parents/carers.

4.4.7 E-mail or text communications between an adult and a pupil outside agreed protocols may lead to disciplinary and/or criminal investigations. This also includes communications through internet based web sites. Internal e-mail systems should only be used in accordance with the school's policy.

4.5 Social contact

4.5.1 Staff should not establish or seek to establish social contact via social media / other communication technologies with pupils for the purpose of securing a friendship or to pursue or strengthen a relationship.

4.5.2 There will be occasions when there are social contacts between pupils and staff, where for example the parent and teacher are part of the same social circle. These contacts however, will be easily recognised and openly acknowledged.

4.5.3 There must be awareness on the part of those working with pupils that some social networking contacts, especially where these are not common knowledge, can be misconstrued as being part of a grooming process. This can also apply to social networking contacts made through outside interests or through the staff member's own family.

4.6 Access to inappropriate images and internet usage

4.6.1 There are no circumstances that will justify adults possessing indecent images of children. Accessing, making and storing indecent images of children is illegal. This will lead to criminal investigation and the individual being barred from working with children, if proven.

4.6.2 Staff should not use equipment belonging to their school/service to access any pornography.

4.6.3 Adults should ensure that pupils are not exposed to any inappropriate images or web links.

4.6.4 Where indecent images of children are found by staff, the police and local authority designated officer (LADO) should be immediately informed.

4.6.5 Where other unsuitable material is found, which may not be illegal but which raises concerns about that member of staff, either HR or the DSL should be informed and advice sought.

5 The use of personal devices in School

5.1 Students- Mobile Device Policy

5.1.1 Introduction

Mobile phones and, in particular, the new generation of smart phones, such as the iPhone, now include many additional functions such as an integrated camera, video recording capability, instant messaging, mobile office applications and mobile access to the internet. These allow immediate access to email, searching for information on the internet and other functions such as access to social networking sites e.g. Facebook, Snapchat, Instagram, Twitter and blogging sites.

For many young people today the ownership of a mobile phone is considered a necessary and vital part of their social life. When used creatively and responsibly the smart phone has great potential to support a student's learning experiences. However, a rise in the number of incidents of misuse of mobile phones in school has created a situation where schools, in conjunction with their Governing Bodies, are implementing a specific set of policy guidelines covering mobile phone use in school.

Bullying, intimidation and harassment are not new in society; however, bullying using a mobile phone represents a new challenge for schools to manage.

Examples of misuse include:

- the deliberate engineering of situations where people's reactions are filmed or photographed in order to humiliate, embarrass and intimidate by publishing to a wider audience such as on Facebook or YouTube

- bullying by text, image and email messaging

- the use of a mobile phone for 'sexting' (the deliberate taking and sending of provocative images or text messages)

- students posting material on social network sites with no thought to the risks to their personal reputation and sometimes with the deliberate intention of causing harm to others

- making disrespectful comments, misrepresenting events or making defamatory remarks about teachers or other students

- general disruption to learning caused by students accessing phones in lessons

- pupils phoning parents immediately following an incident so that the ability of staff to deal with an incident is compromised

- publishing photographs of vulnerable students, who may be on a child protection plan, where this may put them at additional risk

5.1.2 This policy is intended to help Ferndown Upper School make explicit the expectations of the school on student use of mobile phones and the restrictions which are placed on their use in school and on school grounds. This Policy sits alongside the Acceptable Use Policy for Internet Use which all students sign and is shared with parents and carers. They also give clear guidance to staff, students and parents about the consequences for breaches of the Guidelines. The policy should also be read in conjunction with the Keeping Children Safe in Education and Prevent Duty Guidance 2015.

5.1.3 Dealing with breaches of the Guidelines

5.1.3.1 FUS, in agreement with the Governing Body, will agree the sanctions which will apply to the misuse of a mobile phone in school. It is expected that misuse of the mobile phone will be dealt with using the same principles set out in the school behaviour policy, with the response being proportionate to the severity of the misuse.

5.1.3.2 Serious incidents of misuse, particularly where there has been a victim of Cyberbullying will be dealt with by the Heads of Year.

5.1.3.3 Students should be aware that misuse will lead to the confiscation of their mobile phone, communication with parents and the imposition of other sanctions up to and including suspension from school. If the offence is serious it will be reported to the Police.

5.1.3.4 FUS will ensure all staff know the correct procedure to follow where a mobile phone has been confiscated and is not returned to the student at the end of a lesson. This will ensure that the confiscation is correctly recorded and that the phone is kept securely.

5.1.3.5 Where it is deemed necessary to examine the contents of a mobile phone this will be done by a DSL and in line with guidance. The action will be properly recorded in case it later becomes evidence of criminal activity. The record will include the time, who was present and what is found.

5.1.4 Rules for the Acceptable Use of a mobile phone in school by students

Students are allowed to carry their personal mobile phones in school and to use them responsibly in accordance with the following principles:

- Use of the mobile phone during lesson time, including changeover, will only be allowed with the agreement of the teacher and for the explicit purpose of supporting learning. Misuse of this privilege (using the phone for a non-curriculum purpose or any unacceptable use) will result in the confiscation of the phone. The student will be able to collect the phone from the Pastoral / Study Centre at the end of their school day.

- If the phone has been confiscated for serious misuse (see below) the phone will have to be collected by the parent or guardian of the student.

- If a phone goes off in class the student is to be instructed to turn it off. If it goes off again it will be confiscated and sent to Pastoral to be collected at the end of the day.

- Students are not to use the school's ICT facilities or sockets to charge their phones.

- Students in Year 9-11 are not permitted to use their mobile phone in school hours without direct instruction from a staff member to use it. This is from 8.30am to 2.40pm or within an after school activity.

- The security of phone will remain the student's responsibility in all lessons including PE lessons.

- If asked to do so, content on the phone (e.g. messages, emails, pictures, videos, sound files) will be shown to a teacher.

5.1.5 Unacceptable use

The school will consider any of the following to be unacceptable use of the mobile phone and a serious breach of the school's behaviour policy resulting in sanctions being taken.

- Photographing or filming staff or other students without their knowledge or permission

- Photographing or filming in toilets, swimming pools and changing rooms and similar areas

- Using their phone to access inappropriate or offensive sites.

- Bullying, harassing or intimidating staff or students by the use of text, email or multimedia messaging, sending inappropriate messages or posts to social networking or blogging sites

- Refusing to switch a phone off or handing over the phone at the request of a member of staff

- Using the mobile phone outside school hours to intimidate or upset staff and students will be considered a breach of these guidelines in the same way as unacceptable use which takes place in school time.

5.1.6 Sanctions

Students and parents are notified that appropriate action will be taken against those who are in breach of the acceptable use guidelines following the school's behaviour policy. In addition;

- students and their parents should be very clear that FUS is within its rights to confiscate the phone where the guidelines have been breached.

- if a phone is confiscated FUS will make it clear for how long this will be and the procedure to be followed for its return.

- students should be aware that the police will be informed if there is a serious misuse of the mobile phone where criminal activity is suspected

- if a student commits an act which causes serious harassment, alarm or distress to another student or member of staff the ultimate sanction may be permanent exclusion. FUS will consider the impact on the victim of the act in deciding the sanction and parents will be involved.

5.1.7 Confiscation procedure

If a mobile phone is confiscated then:

- the student will be informed that the phone can be collected at the end of school day from the Pastoral Centre.

- FUS will ensure that confiscated equipment is stored in such a way that it is returned to the correct person

- in the case of repeated misuse the phone will only be returned to a parent/carer who will be required to visit the school by appointment to collect the phone. This may be at the end of a week, a half term or longer

- where a student persistently breaches the Guidelines, following a clear warning, the Head Teacher may impose an outright ban from bringing a mobile phone to school. This may be a fixed period or permanent ban.

Where the phone has been used for an unacceptable purpose

- The Head Teacher or a designated staff member will have the right to view files stored in confiscated equipment and will delete any files which are in clear breach of these Guidelines unless these are being preserved as evidence.

- If evidence of the offence is required, this evidence will be preserved by confiscation of the device and keeping it secure or by taking photographs of the screen.

- FUS will consider whether an incident should be reported to the school safeguarding officer.

- The designated staff member should monitor repeat offences to see if there is any pattern in the perpetrator or the victim which needs further investigation.

5.1.7 Support for the Victim and Perpetrator

Where an incident has involved the victimisation, harassment, alarm or distress of another student or member of staff, FUS will provide support for the victim. This should be discussed with the victim's family or where the incident involves a member of staff, appropriate support should be obtained.

To support the rehabilitation of a victim the following support may be offered in consultation with the victim and their family or support person. FUS may:

- follow up with the victim and family and agree a suitable way forward to facilitate an effective closure for the victim to the incident.

- implement our 'restorative practice' procedures. Where the perpetrator agrees, participation in this process will be included as part of their reintegration programme following the incident.

- investigate other avenues to support the victim e.g. Cybermentors or Childline

- ensure that the perpetrator, and any others involved, are educated about the impact of their actions on the victim

- ensure a fully documented case history of the incident is recorded

- provide support in getting any material that may have been posted, removed either through discussion with the poster of the material or contact with the service provider. Help for this can be provided through the LA.

5.1.8 Sixth Form and Access Laptops

A number of Y9-11 students have access to laptops that they either own or lend from the school. From September 2021, Year 12 students will also be allowed a BYOD laptop. These can be used in lessons at the teacher’s discretion.

Laptop users are expected to use their devices in line with all the policy that is applicable to mobile phones as explained in section 5.1. If a student is found to breach this, then sanctions will apply.

5.2 Staff

5.2.1 The user takes full responsibility for his or her device and keeps it with himself/herself at all times or locked away. Whilst the School provides secure lockable lockers for pupils, the School is not responsible for the security (including loss, damage or theft) of any device that is not defined as the property of the School.

5.2.2 School insurance cover will therefore not be applicable or valid. The School would therefore encourage all pupils, staff, volunteers, governors and visitors/guests to extend their home insurance policy under the personal possessions section or alternatively cover electronic devices by a separate policy.

5.2.3 Insurance is, of course, a personal decision, but if pupils, staff, volunteers, governors and visitors/guests choose not to insure such items, please be aware that the School’s insurance policy does NOT cover users’ personal possessions.

5.2.4 If a device is stolen from the School grounds the School will investigate the theft. Wilful damage to devices will also be investigated by the School. Reception must be notified immediately of any incidents and these will be logged.

5.2.5 The user is responsible for the proper care of their personal device, including any costs of repair, replacement or any modifications needed to use the device at School.

5.2.6 Ferndown Upper School takes no responsibility for supporting pupils, staff, volunteers, governors and visitors/guests own devices; nor has the School a responsibility for conducting annual Portable Appliance Testing (PAT) on personally owned devices.

5.2.7 Ferndown Upper School reserves the right to inspect a user's personal device if there is reason to believe that they have violated School policies, administrative procedures, School rules or have engaged in other unacceptable behaviour while using their personal device on School grounds.

5.2.8 Violations of any School policies, administrative procedures or School rules involving a pupil's or staff member's personally owned device may result in the withdrawal of permission to access the School network for individuals or groups at any time and/or may also be subject to disciplinary action.

5.2.9 It is compulsory that any personal device being used to receive or send School e-mail or access to the internet has virus protection software installed and kept up to date. The installation and updating of the software will be the user's responsibility.

5.2.10 For further information, please refer to Appendix B: BRING YOUR OWN DEVICE (BYOD) Frequently Asked Questions (FAQ'S) sheet, included on Page 45 of this policy.

6. Email Protocol and Guidance

6.1 Scope

6.1.1 Section 6 is concerned with setting out the proper and correct us of e-communications infrastructure owned and controlled by Ferndown Upper School. Through this infrastructure, users are able to send and receive email from an individual account.

6.1.2 It applies to all users of Ferndown Upper School's email system, whether through a PC, laptop, personal digital assistant (PDA) or any other hardware device.

6.1.3 It includes Pupils as well as staff and applies equally whether you are working from School, at home or from any other location. These groups of people will thereafter in this document be collectively referred to as users.

6.2 Introduction

6.2.1 Email should be used legally, efficiently, appropriately and securely.

6.2.2 Email senders should be aware of dispatching emails to large numbers of people or copying users into messages unnecessarily. Staff have different work patterns, so while some may be able to respond immediately, others may often be out of the office or spend large parts of their day in meetings.

6.2.3 Equally, email recipients need to manage their inbox effectively, prioritising responses according to their importance, rather than feeling under pressure to reply to all messages immediately.

6.2.4 The purpose of this document is to provide a framework within which email can be used to its full potential within certain parameters. It is divided into two sections; policy (things that you must do when using FUS' email system) and guidance (best practice that you should seek to follow wherever practical).

6.2.5 Usage of email is also covered within the Disciplinary Procedure available from HR and the school Code of Conduct.

6.3 Seeing it from other's point of view

What opinion would you form of an organisation if you contacted them and:

- They responded promptly?
- The reply was clear and fully answered your question?
- The reply was well written in plain English and contained no errors?

- The tone was approachable, non-bureaucratic and polite?

When communicating with the public and each other we will aim to …

- Ensure people are treated with respect, courtesy and understanding
- Be as helpful and open as possible
- Point people in the right direction if we can't help
- Let people know what will happen next

6.4 Email Policy

6.4.1 Users must follow the points below. If there is evidence to suggest that users have failed to abide by these policy requirements, FUS has the right to conduct an investigation. This may result in the removal of your email facility and/or disciplinary action.

6.4.2 FUS retains the right to view all emails sent or received using the corporate email system at any time. Your emails can be intercepted and monitored using powers under the Regulation of Investigatory Powers Act 2000 (RIPA).

6.4.3 Ensure your email account is kept secure by changing your email password regularly and not giving it to anyone.

6.4.4 Users must only use email for business purposes in work time.

6.4.5 Personal use in your own time is acceptable but, in line with the internet filtering policy, use in core time is not permitted, unless in exceptional circumstances you have prior agreement with your line manager.

6.4.6 Any agreed personal use must not make significant demands on IT resources. Therefore, transferring or storing large attachments such as images, audio and video clips is not permitted.

6.4.7 Any personal or business use for illegal, threatening, offensive, obscene, pornographic or libellous purposes is strictly prohibited.

6.4.8 Never use your work email address when posting comments on public bulletin boards or chat rooms unless directly related to your work.

6.4.9 If you receive an email that is obviously spam or of an adult nature, do not open it, rather delete it immediately.

6.4.10 Never participate in chain emails where you are asked to forward an email to a number of others.

6.4.11 In legal terms, under the Telecommunications Regulations 2000, sending an email is as binding as sending a signed letter. Therefore, do not express personal views or information by email, because as an employer, FUS could be held vicariously liable for the opinions and views expressed.

6.4.12 This also applies to comments posted on public discussion boards if you use an FUS email address or state the opinions in a work capacity.

6.4.13 Users can be held criminally liable if they knowingly or recklessly disclose personal information outside the Council's policies and procedures.

6.5 Freedom of Information (FOI) and Data Protection legislation become own section

All emails, regardless of length, are public records. There is no distinction between information contained in an email and any other document.

- Be aware that what you write in an email could become disclosable and therefore available to the public.
- Keep personal information about individuals to a minimum and dispose of that information as soon as the need to use that information has passed.
- FUS may where required use data protection legislation to check users email accounts in their absence. However, if an email is marked 'personal', this will be respected unless there is a business case to do otherwise.
- Under FOI, the public have a right to request information held by the Council, unless it is exempt. It is therefore important that you compose emails with this in mind and that any important emails are stored on shared servers so they can easily be accessed by colleagues if required.
- Check with your data protection officer or IT liaison officer if unsure about any of the above points.

7. Accessibility in Digital Technology

7.1: Physical Disabilities and Impairments

Ferndown Upper School will make adjustments to access of digital devices and services where needed to ensure fair access is given to those with physical disabilities, either staff or students. If this is a staff member this will be arranged by HR, if a student the SENCO.

In the event a student needs specific software and hardware set up, staff may need specific training on how to assist the individual. The SENCO will ensure this training is put into place.

7.2 Educational and Learning Needs

Many students have a learning-needs that may require the use of digital technology in normal lessons or for exam arrangements. The SENCO will ensure that after assessments this provision be made clear in the IEP and put into place where feasible. In some cases this may require financial support from home. The school will do its best to ensure best value for money and provide any hardware for students with financial advice. Pupil premium students may get the devices subsidised or paid for depending on the school's policy at the time regarding this type of assistance.

8. Safeguarding Students and Staff from Digital Technology Risks

8.1 Students

Recognising potential increased risks with students working from home during school closure or isolation periods, the risks assessed below apply to when students and staff are in school and working from home. Any safeguarding issues found regarding young people must be reported and investigated as set out the Child Protection Policy. Section 8.1 outlines specific aspects of threats to children's safety and well-being by Digital Technology and how these may be dealt with. *It is essential that children are safeguarded from potentially harmful and inappropriate online material. An effective whole school and college approach to online safety empowers a school or college to protect and educate pupils, students, and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate.*

8.1.1 Digital awareness and education

As set out in section 2 of this Policy, Students, Parents and Staff will be regularly updated and educated on threats posed by the Digital Space and Technology. This raising of awareness should enable better choices by all parties reducing the risks by any threats posed to students.

8.1.2 Filtering and Monitoring of online content and apps

As set out in previous sections and through KCSIE (p.37), policies implemented will ensure hardware and software solutions minimise the risk posed to students accessing online content that is inappropriate or illegal. However due to the BYOD policy the school cannot take responsibility over content access through 3G/4G or 5G data straight to a student's device. The agreement to the acceptable use policy by parents and students will ensure all parties are aware of their responsibilities in the use of their device during school time.

FUS follows the filtering and monitoring standards from DfE, which includes:

- Identify and assign roles and responsibilities to managed filtering and monitoring systems
- Review filtering and monitoring provision at least annually
- Block harmful and inappropriate content without unreasonably impacting teaching and learning
- Have effective monitoring strategies in place that meet safeguarding needs

FUS Governors review the standards and anything further needed to support the school in meeting these standards

8.1.2 Types of Risks

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

• **content:** being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism. And misinformation, disinformation (including fake news) and conspiracy theories.

• **contact:** being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes'.

• **conduct:** personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying; and

• **commerce** - risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).

The type of behaviours and risks outlined below can overlap one or more of these categories.

8.1.3.1 'Screen Time' (including gaming) , a growing body of research shows that students spend a large proportion of the day on their devices or on computer games. For some students this is reported as up to eight hours. Though the psychological risks posed by this are still debatable it still poses a number of health and social risks.

8.1.3.2 Cyberbullying, Cyberbullying is a growing problem in young people and partly caused by unrestricted and unsupervised access to apps and social media platforms. It is advised that parents heavily monitor students using this and once again school staff can support them doing so.

If a student is the victim of cyberbullying the school will follow the safeguarding policy to evaluate the level of threat. This will be dealt with internally where possible and further advise can be sought from the safer schools team.

8.1.3.3 Grooming, grooming is the act of persuading somebody to change their behaviour to the benefit of the perpetrator. Any person of any gender or age can be a victim or perpetrator of grooming. The victim could be groomed for a variety of reasons including: sexual exploitation, radicalisation or to take financial advantage.

Digital technology has made it much easier for young people to become victims of grooming. This has been made worse by an increase in unsupervised access to various social media apps and platforms.

Any students who is suspected to being groomed (using digital technology or not) will be reported to the safeguarding lead and investigated as required by the Child Protection Policy.

8.1.3.4 **Radical and extremist content**, many young people are at risk of radicalisation. This could be for religious or social ideology. Any students suspected of accessing digital content associated with this must be reported to the safeguarding lead who will follow the Child Protection Policy procedure including referring to PREVENT if deemed appropriate.

The school's digital awareness programme will raise awareness of far right and Islamic extremism and inform students to report any associated activities.

8.1.3.5 **Illicit exchange of media**, with an increase in cameras and audio recording devices it has now become much more common for young people take images of themselves and others. This has unfortunately directly led to the increase in exchanging illicit material known as youth produced sexual imagery (sexting) including 'nude selfies' of children amongst peers and adults. It is illegal to exchange any images or material of this nature (of under age of 18 or under 20 if mentally impaired) by anybody including the young people themselves.

In the assembly rota and the digital awareness programme, this issue is raised with children of all ages across the school. Any children who are found to be victims of this actions will be supported as set out in the Child Protection Policy. Children who exchange this kind of media will be dealt with as required by the school behaviour policy, however intervention by the police may be required if deemed serious enough.

Each case will be dealt with in context and on an individual basis to deem the most appropriate course of action.

8.1.3.6 **Photos and videos**, most students' BYOD have an in-built camera. As part of the acceptable use policy, images should not be taken on site of other children or staff by these devices. Other types of images may be taken with **staff permission**.

If students are found having taken or distributed images taken on site without permission the school will follow the policy as set out in section 5.1 of this document.

8.1.3.7 **Upskirting**. Upskirting typically involves taking a picture under a person's clothing without them knowing, with the intention of viewing their genitals or buttocks to obtains sexual gratification or cause the victim humiliation, distress or alarm. This became an offence under the Voyeurism Act in February 2019. If a student has been a victim of upskirting this may be considering a Sexual Offence.

The school will follow the Child Protection and Behaviour policies to support the victim and take appropriate action against the perpetrator. This has been added to the Digital Awareness program for students and staff to be made aware of.

8.1.3.8 **Social Media & Live Streaming**, as of 2019 the use of Live Streaming has become the biggest threat posed to young people with digital technology. Many apps now have features to enable live broadcasts of themselves to anyone with access to a device.

This poses an increased risk of grooming, sexual exploitation and cyberbullying.

The digital awareness program will raise awareness of risks associated with live streaming and other social media apps to students and parents.

The school recommends that students should not have apps capable of live streaming on their devices. If students are found to be live-steaming video on site they will face a device ban (whilst on school premises) as set out in the mobile device policy.

Any students who are found to be using live streaming regularly (particularly whilst unsupervised) should be reported to their safeguarding lead and investigated. Parents of the child should be spoken to about the risks such software poses.

If a student is found to have been a victim of exploitation via social media or live-streaming the school's Child Protection Policy will be followed and if appropriate, the incident reported to the Police.

8.2 Staff

School staff nationally have seen a rise of online acts against them by the community which can include abuse and false information about them being spread. Ferndown Upper School takes these kinds of acts serious and sets out below how we seek to protect our staff from bullying and harassment.

8.2.1 Malicious use of ICT against staff

8.2.1.1 **Social Media/ online Abuse**, if found by the school (by either the use of software or people reporting directly to us, all aspects of online abuse will be investigated by the Senior Leadership Team.

If the staff member is a victim they will be informed of the act and they have the right to pursue this further if it is deemed serious enough. The school will fully support any actions of staff around this issue.

8.2.1.2 **Illicit exchange of media & Upskirting**, with increased access to devices by students, staff and visitors there is now an increased risk of staff's images and actions being recorded and transferred between people who have such devices. Under the acceptable use policy of staff and students images of staff at work on personal devices are not allowed. If students are found to have taken images or recordings of staff without permission (including upskirting) the school will follow the Student Behaviour policy and put sanctions in place.
If students have been found to exchange material of staff without consent this is deemed a much more serious offence and may result in permanent exclusion.

9. School Digital Infrastructure and Security

Due to the nature of this section the specific details of the school's Digital Security and Infrastructure are not published. However if school leaders or associated Governors have queries regarding aspects of this they can contact the Manager of IT Support.

Ferndown Upper School has various infrastructure in place to minimise the chance of cyberthreats. This includes management of data breaches, viruses, malware, hacking, phishing and other cyber attacks.

9.1 Data Breach

In the event of a reported or suspected breach of data via the digital systems the Data Protection policy will be followed.

9.2 Cyberattacks; DDoS, Hacking

In the event or a reported or suspected cyberattack the systems will be disconnected from the internet where possible and a full evaluation of the impact will be made. The investigation aims for the cause to be found to prevent or reduce the risk of any similar attack in the future.

9.3 Phishing

With a large number of users on our email server there is a significant risk of phishing. Staff and students are regularly updated on the risks posed by suspicious emails, this includes not clicking links which may pose further risks to personal data and IT systems. In the event a phishing email is suspected this must be reported to IT Support.

9.4 Virus/ Malware

The school has various anti-viral software on its systems and to reduce the risk of an infection staff and students should not use memory devices or connect their own mobile devices physically to the network or hardware in school (as set out in the acceptable use policy section).

In the event a virus is suspected or found the device must be taken to IT support who will seek to rectify the issue. All staff and student devices must be kept up to date to minimise such risks.

9.5 Ransom/Blackmail

There is a growing trend of ransomware being installed on networks in public organisations. This software locks files, folders or the whole computer and demands payment. The security methods put in place in school should prevent this from occurring.

In the event this does occur this must be reported to IT support immediately. Under no circumstances should payment be made via the computer or phone. It is likely if it is a work device the files and folders can be recovered by other means. Staff will be updated on any such risks regularly in the Digi-tech termly newsletter.

Appendices

Appendix A: remove

Password Security

Passwords are your protection against your personal, private and business information being compromised and used without your consent. Being hacked can lead to your personal details and those of your friends and colleagues being compromised too. The best defence is herd immunity - everyone keeps everyone else secure.

A common tactic of hackers is to attack an easy password and use that access to gain access to other passwords and so on. This can lead to you're a serious breach of your security and leaking data relating to confidential work. It is your duty and responsibility to take reasonable precautions to protect yourself, your colleagues and the school.

- Do you find passwords hard to remember?
- Do you have password containing names and numbers? Fred99, Janice68 etc.
- Does your password or PIN number contain your date or year of birth?
- Do you have simple passwords of one word and a number?
- Do you use a variant of your username as your password?
- Do you re-use passwords between different sites?
- Do you keep emails with passwords in your email Inbox?

These are all common issues that can be addressed using a simple approach

In theory a 4-number PIN has 9999 different combinations. It has been shown that where people use common sequences such as dates, or repeated numbers (2222, 3333, etc.) these combinations can be reduced to 100s or even 10s. This makes them guessable.

If you use the same PIN number or password for multiple systems then your details can be re-used and access can be gained across different systems. If someone gains access to your email and then resets your password by sending a link to your email then they have access to that system as well. In this way your bank, your social media accounts, your personal and work records can all be accessed.

Hackers will routinely try a list of passwords containing many lists of commonly used passwords in multiple languages, including variations like P@55W0Rd or similar. They can try hundreds of thousands of these a minute with automated systems designed to crack passwords. A short password (7 characters or less) can be hacked in a matter of hours even if it is completely random.

Click the link below for a list of the most commonly used passwords.

http://www.passwordrandom.com/most-popular-passwords

So what can you do?

Making a better password involves:

- It must be hard to deduce or guess
- It must be easy to remember
- It must be easy to enter (on PC, Tablet, Phone)

What if you could have an easy to remember password that is difficult to guess or predict?

Better Passwords

A better password is ten or more characters long and contains numbers, upper and lower case characters and punctuation. You might think this would be difficult to remember but it needn't be:

- Purple.Elephant.H2O
- Zero-Emit-Radio
- Turbo-Fruitcake-365
- Animated.bingo.wins

These are examples of good passwords that are extremely hard to guess but relatively easy to remember and easy to type into a mobile device. With three easy to remember words it is possible to come up with a unique address for every location on the planet, as demonstrated here: http://what3words.com/ . Please do not use your address location for a password as that too would be like using your postcode and is easy to guess for anyone who can look you up.

So using three simple words and a separating character you can easily generate a memorable, easy to use, secure password. You can then have separate passwords for different services you are using so that you don't, for instance, use the same password for the School MIS as you do for Email.

If you have any concerns about network security or would like help changing your password then please feel free to come to IT Support and we will assist.

Appendix B: colin check

BRING YOUR OWN DEVICE (BYOD)

Frequently Asked Questions (FAQ'S)

Q: Is the Bring Your Own Device (BYOD) scheme open to all pupils?
A: The Bring Your Own Device (BYOD) initiative is currently open to all pupils but may be subject to change.

Q: What personal ICT Devices are permitted for use in School by pupils?
A: Pupils can use either a laptop, tablet device, smart phone, chrome-book or any other compatible device that supports the 802.1x wireless standard.

However, should the device be required to run any specialist academic software to assist pupils with their studies (For example; Adobe Premiere Pro for Media Studies) pupils/parents will be advised of any required computer hardware and software specifications separately.

Q: What personal ICT Devices are not permitted for use in School?
A: Computer desktop computers are not permitted to be used as part of the BYOD programme. Any device that does not support the 802.1x wireless standard is not compatible for use on the wireless network.

Q: Can pupils physically plug their devices into the School Network using a network data cable?
A: Pupils should not plug their device, directly into the School network using a network cable. Access to the network can only be permitted via the 'BYOD' wireless network.

Q: How do pupils get permission to use a personal device in School?
A: Both pupils and parents should read and agree to the terms and conditions set out in the Ferndown Upper School ICT Acceptable Use Policy (ICT AUP). Parents and pupils should also familiarise themselves and follow the guidance as outlined in the other linked policies.

Q: Once permission has been provided, how can pupils access the wireless network on their personal device in School?
A: Pupils should connect their device to the 'FUS | Get Connected' wireless network by using their normal School network username and password. And follow instructions in their welcome handbook to get connected.

Q: Does the School provide any ICT technical support for any issues that arise with the pupil's personal devices?
A: Resources will be provided to help pupils connect and understand their device software in relation to the School network. Your child must be familiar with how to use their device. Teachers will incorporate the use of your child's device into learning. However, neither they nor the School will provide technical support with personal hardware.

Q: Do I have to buy something now?
A: No. Your son/daughter can bring their device anytime up until the time they leave the School. There is no time-limit on when they might want to log into the network.

Q: Are pupil personal devices insured under the School's insurance policy?

A: No. The pupil takes full responsibility for his or her device and keeps it with himself or herself at all times or locked away. Whilst the School provides secure lockable lockers, the school is not responsible for the security (Including loss, damage or theft) of any device that is not defined as the property of the School.

School insurance cover will therefore not be applicable or valid. The school would therefore encourage all parents to extend their home insurance policy under the personal possessions section or alternatively cover electronic devices by a separate policy.
Insurance is, of course, a personal decision, but if parents choose not to insure such items please be aware that the school's insurance policy does NOT cover pupils' personal possessions.

If a device is stolen from the school grounds the school will investigate the theft. Wilful damage to devices will also be investigated by the school. Reception must be notified immediately of any incidents and these will be logged.

Q: How can pupils charge their ICT devices at school?
A: Devices should be charged at home. All electrical devices used in school need to be Portable Appliance Tested (PAT) so, for Health and Safety reasons, personal devices cannot be charged in School.

Q: Can pupils use their own personal ICT device in class?
A: We expect our Sixth Form students to work off a personal ICT device in most their lessons. For Year 9-11, devices may only be used in class with the approval of the class teacher / SENCO.

Q: Can pupils use their device as a personal Wi-Fi Hotspot or broadcast their own wireless network to allow others to access the internet?
A: Pupils are not permitted to use their device to broadcast their own SSID or use it as a 'Hotspot' so that it can allow others to access the internet by by-passing the School's wireless network whilst in School.

The School will not be responsible for any content accessed by a user using their own devices through non-School controlled wireless systems such as personal 3G and 4G networks, 'Hotspots', Proxy or VPN bypass Systems.

Ferndown Upper School cannot permit access to non-filtered services for safety reasons and this includes all wireless services. Any pupil enabling such a network would be committing a gross breach of trust that could result in them no longer being able to use a personal ICT device in School. Additional sanctions for breaching School rules could also apply.

Q: Why are pupils filtered and monitored on their own device? Shouldn't they be able to see what they want to on their own device?
A: The School is providing pupils with a service, whilst being committed to making sure the network is safe and secure as possible. This is also part of our wider duty of care. Any personal device using the School's wireless network is filtered, monitored and secured according to policy. Please note, the 'BYOD' wireless network is there to help support teaching and learning and not as a recreational tool.

The School will not be responsible for any content accessed by a user using their own devices through non-School controlled wireless systems such as personal 3G and 4G networks, 'Hotspots', Proxy or VPN bypass/avoidance Systems.

Q: Can pupils still study adequately without a laptop/device?
A: Absolutely. The School has many rooms and areas where pupils can access computers before, during and after the School day. Additionally, if access to devices is required for a particular lesson, teachers will book School devices. Quality learning can also take place without the need for technology. This is an opt-in policy; where pupils feel more comfortable with technology they can use it. However, traditional approaches to learning are still appropriate and, importantly, work.

Q: Can pupils access any School specific teaching and learning software including their school network data files from their personal device?

A: Pupils can access a range their School Document files from their personal computer devices via the School's secure software application portal - accessible via https://hap.fernup.dorset.sch.uk/

Pupils can also now login with their normal School network username and password and use Office 365 online – accessible via the school website

Office 365 offers the following benefits for the pupils:

- Accessible from any computer with an Internet connection and also works across a range of mobile devices.
- Ability to create and store up to 1TB of data files into your OneDrive Data area using the Microsoft online apps for Word, Excel, PowerPoint and OneNote (no software installation necessary).
- Office 365 ProPlus. This is the option to install the full version of Microsoft Office on up to 5 devices (PCs or Apple Mac's); and Office Mobile on up to 5 mobile devices completely free of charge. This option will be available to all current Ferndown Upper School pupils whilst they are registered with the School.

Appendix C: Students/ Parents Acceptance of Policy

Provided by parents/legal guardians and pupils

I/We as the parents/legal guardians give the following express authorities on behalf of myself/ourselves and (so far as I am entitled to do so) on behalf of my/our child:

- As a pupil and parent I understand that this ICT Acceptable Use Policy (ICT AUP) applies not only to the pupil's work and use of School ICT equipment in School, but also applies to the use of School ICT systems and equipment on and off the premises.

- Where own personal devices in School will be used, the pupil will take full responsibility for their device and keep it with them at all times or locked away. Pupils are also fully aware that the School is not responsible for the security (Including loss, damage or theft) of any device that is not defined as the property of the School and if they or the Parent/legal guardians choose not to insure such items separately the School's insurance policy does NOT cover any personal possessions.

- As a pupil, I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action.

- I also give permission for any activities undertaken by me regarding network/Internet transactions and access to be monitored and logged and kept for an appropriate amount of time.

- I am aware that logs are taken for reasons of security, diagnostic and account/audit purposes and these logs are available only to authorised members of staff and kept for no longer than necessary and in line with current Data Protection guidelines.
  Such records and information are sometimes required - under law - by external agencies and authorities. ICT Services/Support will comply with such requests when and if they are formally submitted.

As a pupil and parent I have read and understand the above (together with any linked policies) and agree to use the School/Trust ICT systems (both in and out of School) and my own devices (in School and when carrying out communications related to the School) set out within these guidelines.

Both parents and pupils must provide consent and acceptance of the ICT Acceptable Use Policy and Online Safety Policy online/electronically by replying to and viewing the email and attachments that will be sent to parents separately via the School's Post-Modern Online Communication System with the email subject message: Ferndown Upper School ICT Acceptable Use Policy (ICT AUP) and Online Safety
Policy.

A permanent copy of the email message including policy documents and consent form will be stored, accessible and searchable from within the parent's individual Post-Modern 'mailbox'.

Appendix D: Staff Acceptance of Policy

Provided by staff, volunteers, governors and visitors/guests

- As a member of staff, volunteer, governor and/or visitor/guest I understand that this ICT Acceptable Use Policy (ICT AUP) applies not only to my work and use of School ICT equipment in School, but also applies to the use of School/Trust ICT systems and equipment on and off the premises.

  Where own personal devices in School will be used, the user will take full responsibility for their device and keep it with them at all times or locked away. Users are also fully aware that the School is not responsible for the security (Including loss, damage or theft) of any device that is not defined as the property of the School and if they choose not to insure such items separately the School's insurance policy does NOT cover any personal possessions.

- As a member of staff, volunteer, governor and/or visitor/guest, I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action.

- I also give permission for any activities undertaken by me regarding network/Internet transactions and access to be monitored and logged and kept for an appropriate amount of time.

- I am aware that logs are taken for reasons of security, diagnostic and account/audit purposes and these logs are available only to authorised members of staff and kept for no longer than necessary and in line with current Data Protection guidelines.

  Such records and information are sometimes required - under law - by external agencies and authorities. ICT Services/Support will comply with such requests when and if they are formally submitted.

As a member of staff, volunteer, governor and/or visitor/guest I have read and understand the above (together with any linked policies) and agree to use the School/Trust ICT systems (both in and out of School) and my own devices (in School and when carrying out communications related to the School) set out within these guidelines.

All staff <u>must</u> provide consent and acceptance of the ICT Acceptable Use Policy and Online Safety Policy online/electronically by replying to and viewing the email and attachments that will be sent to staff separately via the School's Post-Modern Online Communication System with the email subject message:
Ferndown Upper School ICT Acceptable Use Policy (ICT AUP) and Online Safety
Policy.

A permanent copy of the email message including policy documents and consent form will be stored, accessible and searchable from within the staff member's individual Post-Modern 'mailbox'.

Appendix E - Guidance on Confiscation

"Schools' general power to discipline, as set out in Section 91 of the Education and Inspections Act 2006, enables a member of staff to confiscate, retain or dispose of a pupil's property as a disciplinary penalty, where reasonable to do so."

For full document http://www.education.gov.uk/schools/pupilsupport/behaviour/f0076897/screening

DfE Behaviour and discipline guidance for school staff

http://media.education.gov.uk/assets/files/pdf/b/behaviour%20and%20discipline%20in%20schools%20%20%20guidance%20for%20teachers%20and%20school%20staff.pdf

Appendix F- Police response to an incident in school

Extract from the Home Office guidance on the action police should take if a crime may have occurred in school.

In order to sustain the disciplinary authority of schools, this guidance clarifies the general principles of NCRS as they apply specifically to incidents on school premises. When police have reported to them an incident which took place on school premises, including those witnessed by, or reported directly to, officers working in the school, which they would normally record as a notifiable offence will, in the first instance, invite the victim or the person acting on their behalf to report the matter to the head teacher to be dealt with under normal school discipline procedures. Such reports should be recorded as an incident only, until or unless:-

(a) they judge it to be a serious incident as defined below; [see full document]

(b) having brought the matter to the attention of the school in line with good practice (see references to guidance papers below), they receive a formal request from the school to create a crime record; or

(c) the child, parent or guardian or the child's representative asks the police to create a crime record.

For full description see Annex E in following document: Crime Recording by Police Officers working in Schools. http://www.homeoffice.gov.uk/publications/science-research-statistics/research-statistics/crime-research/counting-rules/count-recstan?view=Binary

Appendix G – Relevant legislation

Schools staff should be aware of the legislative framework which currently surrounds use of social media / communication technology in the UK. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

- Voyeurism (Offences) Act 2019
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- DfE (2024) 'Filtering and monitoring standards for schools and colleges'
- DfE (2021) 'Harmful online challenges and online hoaxes'
- DfE (2024) 'Keeping children safe in education 2024'
- DfE (2023) 'Teaching online safety in school'
- DfE (2022) 'Searching, screening and confiscation'
- DfE (2023) 'Generative artificial intelligence in education'
- Department for Science, Innovation and Technology and UK Council for Internet Safety (2024) 'Sharing nudes and semi-nudes: advice for education settings working with children and young people'
- UK Council for Child Internet Safety (2020) 'Education for a Connected World – 2020 edition
- National Cyber Security Centre (2020) 'Small Business Guide: Cyber Security'

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

Appendix H – Updated information and support

There is a wealth of information available to support schools, colleges and parents/carers to keep children safe online. The following list is not exhaustive but should provide a useful starting point all include website links:

Advice for governing bodies/proprietors and senior leaders

• Childnet provide guidance for schools on cyberbullying

• Educateagainsthate provides practical advice and support on protecting children from extremism and radicalisation

• London Grid for Learning provides advice on all aspects of a school or college's online safety arrangements

• NSPCC provides advice on all aspects of a school or college's online safety arrangements

• Safer recruitment consortium "guidance for safe working practice", which may help ensure staff behaviour policies are robust and effective

• Searching screening and confiscation is departmental advice for schools on searching children and confiscating items such as mobile phones

• South West Grid for Learning provides advice on all aspects of a school or college's online safety arrangements

• Use of social media for online radicalisation - A briefing note for schools on how social media is used to encourage travel to Syria and Iraq

• UK Council for Internet Safety have provided advice on, and an Online Safety Audit Tool to help mentors of trainee teachers and newly qualified teachers induct mentees and provide ongoing support, development and monitoring

• Department for Digital, Culture, Media & Sport (DCMS) Online safety guidance if you own or manage an online platform provides practical steps on how companies can embed safety into the design of their online platforms. It offers information on common platform features and functions (such as private messaging) and their risks, as well as steps that can be taken to manage that risk.

• Department for Digital, Culture, Media & Sport (DCMS) A business guide for protecting children on your online platform provides guidance to businesses on how to protect children on their online platform. It outlines existing regulatory requirements and provides best practice advice on how to protect children's

- personal data, ensure content is appropriate for the age of users, ensure positive user-to-user interactions and address child sexual exploitation and abuse.

Remote education, virtual lessons and live streaming

- Case studies on remote education practice are available for schools to learn from each other
- Departmental guidance on safeguarding and remote education including planning remote education strategies and teaching remotely
- London Grid for Learning guidance, including platform specific advice
- National cyber security centre guidance on choosing, configuring and deploying video conferencing
- National cyber security centre guidance on how to set up and use video conferencing
- UK Safer Internet Centre guidance on safe remote learning

Support for children

- Childline for free and confidential advice
- UK Safer Internet Centre to report and remove harmful online content
- CEOP for advice on making a report about online abuse

Parental support

- Childnet offers a toolkit to support parents and carers of children of any age to start discussions about their online life, to set boundaries around online behaviour and technology use, and to find out where to get more help and support
- Commonsensemedia provide independent reviews, age ratings, & other information about all types of media for children and their parents
- Government advice about protecting children from specific online harms such as child sexual abuse, sexting, and cyberbullying
- Government advice about security and privacy settings, blocking unsuitable content, and parental controls
- Internet Matters provide age-specific online safety checklists, guides on how to set parental controls on a range of devices, and a host of practical tips to help children get the most out of their digital world
- Let's Talk About It provides advice for parents and carers to keep children safe from online radicalisation
- London Grid for Learning provides support for parents and carers to keep their children safe online, including tips to keep primary aged children safe online
- Stopitnow resource from The Lucy Faithfull Foundation can be used by parents and carers who are concerned about someone's behaviour, including children who may be displaying concerning sexual behaviour (not just about online)
- National Crime Agency/CEOP Thinkuknow provides support for parents and carers to keep their children safe online
- Net-aware provides support for parents and carers from the NSPCC and O2, including a guide to social networks, apps and games
- Parentzone provides help for parents and carers on how to keep their children safe online
- Parent info from Parentzone and the National Crime Agency provides support and guidance for parents from leading experts and organisations
- UK Safer Internet Centre provide tips, advice, guides and other resources to help keep children safe online